# INVALIDATION REPORT

## US-9251332-B2

**Patent Title:**

Security system and method for controlling access to computing resources

**Report Generation Date:**

12 August 2025

**Priority Date:**

19 Dec 2007

# Summary of Subject Patent

The invention is a security system that uses a personal digital key (PDK), a reader, and a computing device to control access to digital resources. The PDK is a portable transceiver containing passwords or codes, which communicates with the reader to verify the user's presence. The computing device includes a detection engine that monitors file access and third-party system interactions, granting or denying access based on whether the PDK is linked to the reader. This system enhances security by ensuring that only users with the authorized PDK can access the device's functions. Additionally, the invention provides methods for initializing the system, setting up the computing device, and managing access control.

## Relevance Ranking - Patents

## Relevance Ranking - Non-Patent Literature

# Patent Literature

This section presents a collection of patent documents sourced from Google Patents that are relevant to the subject patent. These references provide additional insights that may contribute to a broader understanding or assessment of the invention.

**Rank 1:** US-11562644-B2 **Priority Date:** 2007-11-09

**Assignee:** Proxense; Llc

**Inventor(s):** David L. Brown

**Patent Reference:** https://patents.google.com/patent/US11562644B2

## Similarity Analysis:

US-11562644-B2 discloses a system and method involving a personal digital key (PDK) detected within a proximity zone of a sensor, with wireless communication to authenticate and control access to applications, including automatic logout when the PDK leaves the proximity zone. US-9251332-B2 describes a more comprehensive security system with a PDK linked wirelessly to a reader, controlling access to computing resources based on security setup data stored in encrypted memory, including user-defined security actions like biometric confirmation and exit-based rules. While both involve PDK proximity detection and access control, US-9251332-B2 includes additional features such as dedicated encrypted security setup data, biometric confirmation, and a more detailed security system controlling multiple computing resources. US-11562644-B2 focuses on login/logout to applications based on proximity and authentication. Thus, US-11562644-B2 captures some but not all aspects of Claim-1 in US-9251332-B2, leading to a 'Maybe' on similarity.

## Anticipation Analysis:

US-11562644-B2 does not explicitly disclose all elements of Claim-1 of US-9251332-B2, particularly the dedicated encrypted portion of memory storing security setup data excluding the security data, user-defined options for different security actions including biometric confirmation, and the detailed control of multiple computing resources. US-11562644-B2 focuses on proximity detection and automatic login/logout to applications but lacks the comprehensive security setup and control features of US-9251332-B2. Therefore, US-11562644-B2 does not anticipate US-9251332-B2 as it does not disclose all claim elements either expressly or inherently.

## Novelty Analysis:

US-9251332-B2 is novel over US-11562644-B2 because it introduces unique features not found in US-11562644-B2, such as the dedicated encrypted memory portion storing security setup data separate from security data, user-configurable security actions for different computing resources, and biometric confirmation as a security action. US-11562644-B2's disclosure of proximity-based

login/logout and authentication does not encompass these novel aspects, preserving the novelty of US-9251332-B2.

### Obviousness Analysis:

Some elements of Claim-1 in US-9251332-B2, such as proximity detection of a PDK and controlling access based on authentication, are present in US-11562644-B2 and could be considered obvious extensions. However, the inclusion of dedicated encrypted security setup data, user-defined security actions including biometrics, and exit-based rules for terminating access represent additional inventive steps. Whether these are obvious in light of US-11562644-B2 depends on the level of ordinary skill and motivation to combine these features, leading to a 'Maybe' on obviousness.

### Additional Prior Art from the Same Patent Family:

Apart from US-11562644-B2 whose claim chart is provided below, US-9728080-B1, US-8659427-B2, US-10769939-B2, US-2023146442-A1 also belong to the same patent family. These may also aid in the invalidation of the subject patent. These patents disclose similar technical features and concepts that are relevant to the claims of the subject patent, potentially impacting its novelty and inventive step.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-11562644-B2 | Status | Explanation |
|---|---|---|---|---|
| 1 | "a **personal digital key** adapted for **wireless communication** within a **predefined range** to establish a link and send and receive data," | "detecting a **personal digital key (PDK)** within a **proximity zone** of a sensor; responsive to the detecting, initiating **wireless transmission** of a request including an access key for login information from the PDK (Claim 1)" | Match | Both patents disclose a PDK capable of wireless communication within a predefined range to establish a link and exchange data. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-11562644-B2 | Status | Explanation |
|---|---|---|---|---|
| 2 | "the **personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by security set up data for the particular computing resource;" | "the **access key being unique to an application** that **unlocks the login information stored in the PDK** (Claim 1)" | Partial | US-11562644-B2 discloses security data (login information) stored in the PDK, but does not explicitly describe association with particular computing resources or security setup data as in US-9251332-B2. |
| 3 | "a **reader** for **automatically detecting the presence of the personal digital key** and establishing a link with the personal digital key," | "a sensor device including a **reader device** that **detects a personal digital key** within a proximity zone (Claim 13)" | Match | US-11562644-B2 discloses a reader device that automatically detects the presence of the PDK and establishes communication. |
| 4 | the reader having an input and an output and adapted for **wireless communication with the personal digital key** when the reader and the personal digital key are within the predefined range of each other, | **initiating wireless transmission** of a request including an access key for login information from the PDK (Claim 1) | Match | US-11562644-B2 discloses wireless communication between the reader and PDK within a proximity zone. |
| 5 | the reader **automatically signaling a computing device whether it is linked to the personal digital key**; | **responsive to verification of the login information from the PDK**, logging a user into the application (Claim 1) | Partial | US-11562644-B2 implies signaling and control based on PDK presence but does not explicitly describe signaling a computing device about link status as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-11562644-B2 | Status | Explanation |
|---|---|---|---|---|
| 6 | the **computing device** having **computing resources** including the particular computing resource, | **enabling access** to the **application** responsive to verifying authentication information from the PDK (Claim 7) | Partial | US-11562644-B2 enables access to applications but does not explicitly describe multiple computing resources as in US-9251332-B2. |
| 7 | "the **computing device** **coupled to the input and the output of the reader** for **sending and receiving data**;" | "the **sensor device** including a **reader device** and memory including instructions for **wireless communication** with the PDK (Claim 13)" | Match | US-11562644-B2 discloses coupling between the sensor/ reader and computing device for data exchange. |
| 8 | the computing device including **a security system for controlling access to the computing resources of the computing device** based on **security set up data**, | responsive to **verification of the login/authentication information** from the PDK, **enabling or disabling access to the application** (Claims 1,7,13,19) | Partial | US-11562644-B2 controls access based on authentication but does not disclose a security system using security setup data as in US-9251332-B2. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | receiving the login/authentication information from a secure memory element of the PDK (Claims 2,8,14,20) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-11562644-B2 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | | Not Found | |
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | | Not Found | |
| 12 | the **security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key**, | **responsive to determining that the PDK is no longer within the proximity zone of the sensor device, automatically logging the user out or disabling access** (Claims 1,7,13,19) | Partial | US-11562644-B2 discloses automatic logout or disabling access when PDK leaves proximity, but does not explicitly describe control by a signal indicating link status. |
| 13 | and **terminating access to the computing resource** based on an exit-based rule of the security set up data associated with the computing resource when the **personal digital key and the reader are no longer within the predefined range**. | **responsive to determining that the PDK is no longer within the proximity zone of the sensor device**, **automatically logging the user out of the application or disabling access** (Claims 1,7,13,19) | Match | US-11562644-B2 discloses automatic termination of access when the PDK leaves the proximity zone, matching the exit-based rule concept. |

**Rank 2:** US-20080040609-A1 **Priority Date:** 2004-03-08

**Assignee:** Proxense; Llc

**Inventor(s):** John Giobbi

**Patent Reference:** https://patents.google.com/patent/US20080040609A1

## Similarity Analysis:

US-20080040609-A1 discloses a personal digital key capable of wireless communication with a reader/decoder circuit integrated with a computer, and authentication of access to computer readable media. However, US-20080040609-A1 lacks explicit mention of a dedicated encrypted memory storing security setup data separate from the security data, user-defined options for different security actions, biometric confirmation, and exit-based rules for terminating access based on proximity. US-20080040609-A1 captures the general concept of a personal digital key and reader system for access control but does not clearly disclose the detailed security setup data management and biometric and exit-based control features of US-9251332-B2. Thus, US-20080040609-A1 partially overlaps but does not fully capture all aspects of Claim-1 of US-9251332-B2.

## Anticipation Analysis:

US-20080040609-A1 does not explicitly or inherently disclose the dedicated encrypted portion of memory storing security setup data excluding security data, user-defined options for different security actions including biometric confirmation, or exit-based rules for terminating access when the personal digital key is out of range. These features are critical elements of Claim-1 in US-9251332-B2. Therefore, US-20080040609-A1 does not anticipate US-9251332-B2 as it lacks these specific structural and functional elements.

## Novelty Analysis:

US-9251332-B2 introduces novel elements such as the dedicated encrypted memory portion for security setup data excluding security data, user-configurable security actions including biometric confirmation, and exit-based rules for terminating access based on proximity of the personal digital key and reader. These features are not disclosed or suggested in US-20080040609-A1, which only broadly covers a personal digital key and reader system for authentication. Hence, US-9251332-B2 is novel over US-20080040609-A1.

## Obviousness Analysis:

While US-20080040609-A1 discloses a personal digital key and reader system for authentication, the specific features of dedicated encrypted security setup data, user-defined security actions including biometrics, and exit-based access termination are not disclosed. However, these could be considered obvious extensions or improvements to the general concept of a personal digital key system for access control. A person skilled in the art might find it obvious to implement these features based on US-20080040609-A1's disclosure, but this is not conclusively shown. Therefore, obviousness is uncertain and requires further analysis.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080040609-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | "a **personal digital key** adapted for **wireless communication** within a predefined range to establish a link and send and receive data," | "The **personal digital key** is a tangible object, capable of **wireless communication** with the reader/decoder circuit. (Claim 2)" | Match | Direct correspondence in functionality and implementation of wireless communication between personal digital key and reader. |
| 2 | **the personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by security set up data for the particular computing resource; | A **personal digital key** stores **information unique to the user and authenticates access to computer readable medium**. (Claim 1, 16) | Partial | US-20080040609-A1 discloses storing user-specific information but does not explicitly describe security setup data for particular computing resources. |
| 3 | "a **reader** for **automatically detecting the presence of the personal digital key** and **establishing a link with the personal digital key**," | "**Reader**/decoder circuit capable of **wireless communication** with **personal digital key**. (Claim 2)" | Match | Strong match as reader automatically detects and links with personal digital key. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080040609-A1 | Status | Explanation |
|---|---|---|---|---|
| 4 | "the **reader** having an input and an output and adapted for **wireless communication with the personal digital key** when the **reader** and the personal digital key are within the predefined range of each other," | "**Reader**/decoder circuit integrated with computer and **communicates wirelessly with personal digital key**. (Claim 3, 10)" | Match | Reader has input/ output and wireless communication within range as described. |
| 5 | the **reader** automatically signaling a computing device whether it is linked to the **personal digital key**; | Computer authenticates user based on data from **personal digital key** via **reader**/decoder circuit. (Claim 1, 13) | Partial | US-20080040609-A1 implies signaling for authentication but does not explicitly describe automatic signaling of link status to computing device. |
| 6 | the **computing device** having **computing resources** including the **particular computing resource**, | **Computer** with **hard drive** and **computer readable medium** accessible upon authentication. (Claim 3, 1) | Match | Computing device with resources accessible upon authentication is disclosed. |
| 7 | "the **computing device** coupled to the **input and the output** of the reader for **sending and receiving data**;" | "**Reader/decoder circuit** integrated with **computer** hard drive enabling **data transfer**. (Claim 3, 10)" | Match | Direct correspondence in coupling and data exchange between reader and computing device. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080040609-A1 | Status | Explanation |
|---|---|---|---|---|
| 8 | the computing device including **a security system for controlling access** to the computing resources of the computing device based on **security set up data**, | **System authenticates access** to computer readable medium using **personal digital key data**. (Claim 1, 16) | Partial | US-20080040609-A1 discloses access control but does not specify use of security setup data distinct from security data. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | | Not Found | |
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080040609-A1 | Status | Explanation |
|---|---|---|---|---|
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | | Not Found | |
| 12 | the **security system controlled by the signal from the reader** indicating whether the **reader is linked to the personal digital key**, | **Authentication depends on data from personal digital key via reader**. (Claim 1, 13) | Partial | US-20080040609-A1 implies control based on authentication signal but does not explicitly describe control by link signal from reader. |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | | Not Found | |

**Rank 3:** US-20060136742-A1 **Priority Date:** 2000-12-27

**Assignee:** Giobbi John J

**Inventor(s):** John Giobbi

**Patent Reference:** https://patents.google.com/patent/US20060136742A1

## Similarity Analysis:

US-20060136742-A1 discloses a personal digital key and a receiver/decoder circuit system that automatically authenticates the key based on proximity, enabling linking to an account. This overlaps with US-9251332-B2's personal digital key and reader establishing a wireless link within a predefined range. However, US-9251332-B2 uniquely includes a computing device with a security system controlling access based on encrypted security setup data with user-defined options including biometric confirmation and exit-based rules for terminating access. US-20060136742-A1 focuses on authentication and account linking but does not explicitly disclose the detailed security setup data, user-defined security actions, or biometric confirmation features of US-9251332-B2. Thus, US-20060136742-A1 captures some but not all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20060136742-A1 anticipates the concept of a personal digital key communicating wirelessly within a range to a receiver and authenticating based on proximity. However, it does not explicitly or inherently disclose the security setup data stored in a dedicated encrypted portion of the computing device memory, the user-defined security actions including biometric confirmation, or the exit-based rule for terminating access when the key is out of range. These features are critical elements of Claim-1 in US-9251332-B2 and are not found in US-20060136742-A1, so US-20060136742-A1 does not anticipate US-9251332-B2.

## Novelty Analysis:

US-9251332-B2 is novel over US-20060136742-A1 because it introduces a security system controlling access to computing resources based on encrypted security setup data with user-configurable security actions, including biometric confirmation and exit-based rules for access termination. US-20060136742-A1 primarily addresses automatic authentication and account linking based on proximity but lacks these detailed security control features. Therefore, the novelty of US-9251332-B2 is not invalidated by US-20060136742-A1.

**Obviousness Analysis:**

While US-20060136742-A1 discloses automatic authentication of a personal digital key based on proximity, extending this to a security system controlling access to computing resources with encrypted setup data and user-defined security actions including biometrics could be considered an obvious enhancement to one skilled in the art. However, the specific implementation of exit-based rules and biometric confirmation may not be straightforward or suggested explicitly in US-20060136742-A1. Hence, obviousness is uncertain and requires further analysis.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060136742-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a **personal digital key** adapted for **wireless communication** within a predefined range to establish a link and send and receive data, | The **personal digital key** transmits the unique encrypted digital data to the receiver/decoder circuit through a secure **wireless link**. | Match | Direct correspondence in wireless communication within a range to establish a link and exchange data. |
| 2 | "the **personal digital key** associated with a user and **storing security data used to access a particular computing resource** as described by security set up data for the particular computing resource;" | "The **personal digital key** includes encrypted digital data unique thereto, enabling **automatic authentication and linking to an account associated with a person**. (Abstract, Claim 1)" | Partial | US-20060136742-A1 associates the key with a person and stores encrypted data, but does not explicitly disclose storing security data for accessing particular computing resources as described by security setup data. |
| 3 | "a **reader for automatically detecting the presence of the personal digital key** and **establishing a link with the personal digital key**," | "The **receiver/decoder circuit is able to detect**, authenticate, and securely communicate with the **personal digital key**. (Claim 7)" | Match | Strong match in automatic detection and establishing communication link. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060136742-A1 | Status | Explanation |
|---|---|---|---|---|
| 4 | the reader having **an input and an output** and adapted for **wireless communication with the personal digital key** when the reader and the personal digital key are within the predefined range of each other, | The personal digital key transmits the unique encrypted digital data to the **receiver/decoder circuit** through a **secure wireless link**. (Claim 4) | Match | Direct match in wireless communication within range between reader and key. |
| 5 | the reader **automatically signaling a computing device whether it is linked to the personal digital key**; | The **linked account is unlocked upon the personal digital key being located in proximity to the receiver/decoder circuit, and locked upon being out of proximity**. (Claim 13) | Partial | US-20060136742-A1 signals account lock/unlock based on proximity, similar to signaling link status, but does not explicitly mention signaling a computing device about link status. |
| 6 | "the **computing device** having **computing resources** including the **particular computing resource**," | "The system includes a **computer** with a **computer hard drive**, wherein the receiver/decoder circuit is located in the **computer hard drive**. (Claim 48)" | Partial | US-20060136742-A1 discloses a computing device with receiver/ decoder circuit but does not detail computing resources including particular resources as in US-9251332-B2. |
| 7 | "the **computing device** coupled to the **input and the output** of the reader for **sending and receiving data**;" | "The **computer** or included as a card. The **receiver/decoder circuit** is integrated with the **receiver/ decoder circuit**." | Match | Strong match in coupling the reader to the computing device for data communication. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060136742-A1 | Status | Explanation |
|---|---|---|---|---|
| 8 | the computing device including a security system for controlling access to the computing resources of the computing device based on security set up data, | US-20060136742-A1 discloses authentication and account linking but does not explicitly disclose a security system controlling access based on security setup data stored in encrypted memory. | Not Found | |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | No explicit disclosure of security setup data stored in dedicated encrypted memory excluding security data used for access. | Not Found | |
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | No disclosure of user-defined options for different security actions for different computing resources. | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060136742-A1 | Status | Explanation |
|---|---|---|---|---|
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | No disclosure of biometric confirmation as a security action. | Not Found | |
| 12 | "the **security system controlled by the signal from the reader** indicating whether the reader is linked to the personal digital key," | "US-20060136742-A1 discloses **unlocking/locking linked account based on proximity signal from receiver/decoder circuit**, which is similar but not explicitly controlling a security system for computing resources." | Partial | Similar concept of control based on proximity signal but lacks explicit control of security system for computing resources. |
| 13 | "and **terminating access to the computing resource** based on an exit-based rule of the security set up data associated with the computing resource when the **personal digital key and the reader are no longer within the predefined range**." | "US-20060136742-A1 discloses **locking the linked account** when the **personal digital key is out of proximity**. (Claim 13)" | Partial | Similar concept of terminating access based on proximity but lacks detailed exit-based rule as in US-9251332-B2. |

**Rank 4:** US-20090036164-A1 **Priority Date:** 2007-08-02

**Assignee:** Red Hat; Inc.

**Inventor(s):** Peter A. Rowley

**Patent Reference:** https://patents.google.com/patent/US20090036164A1

## Similarity Analysis:

US-20090036164-A1 discloses a wireless transceiver device (e.g., smart card or cellular phone) that communicates over a personal area network (PAN) to authenticate a user to a computing device, allowing access upon authentication. US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to establish a link with a reader, which signals a computing device to control access to computing resources based on security setup data. Both involve wireless authentication and access control. However, US-9251332-B2 uniquely includes a dedicated encrypted memory portion storing security setup data excluding the security data itself, user-defined security actions including biometric confirmation, and exit-based rules terminating access when the PDK leaves range. US-20090036164-A1 does not explicitly disclose these user-defined security actions, biometric confirmation, or dedicated encrypted setup data separate from security data. Thus, US-20090036164-A1 captures some but not all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20090036164-A1 anticipates wireless authentication and access control via a personal area network using a portable device storing user credentials (digital certificate). However, it does not explicitly or inherently disclose the dedicated encrypted portion of memory storing security setup data separate from security data, user-defined options for different security actions per resource, biometric confirmation, or exit-based rules for terminating access based on proximity. These elements are critical in Claim-1 of US-9251332-B2 and are not found in US-20090036164-A1, so US-20090036164-A1 does not anticipate US-9251332-B2.

## Novelty Analysis:

US-9251332-B2 is novel over US-20090036164-A1 because it introduces a unique combination of features: a dedicated encrypted memory portion storing security setup data excluding the security data, user-configurable security actions including biometric confirmation, and automatic termination of access based on exit-based rules when the personal digital key leaves range. US-20090036164-A1 lacks these specific features and focuses mainly on wireless authentication

using a digital certificate and automatic logoff upon disconnection, which is insufficient to invalidate the novelty of US-9251332-B2.

### Obviousness Analysis:

While US-20090036164-A1 discloses wireless authentication and automatic logoff upon disconnection, the specific features of US-9251332-B2 such as dedicated encrypted setup data excluding security data, user-defined security actions including biometrics, and exit-based rules for access termination are not explicitly disclosed. These could be considered obvious extensions to someone skilled in the art to enhance security, but the absence of explicit disclosure and the specific combination in US-9251332-B2 means obviousness is uncertain without further evidence.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20090036164-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a **personal digital key adapted for wireless communication within a predefined range** to establish a link and **send and receive data**, | a **wireless transceiver to communicatively couple to a personal area network (PAN)** to **receive** an authentication request via the PAN from a device; (Claim 1) | Match | Both disclose a portable device with wireless communication capabilities within a defined range to establish a link for authentication. |
| 2 | the **personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by security set up data for the particular computing resource; | a **storage device** coupled to the wireless transceiver to store **a digital certificate that uniquely identifies a user**; (Claim 1) | Partial | US-20090036164-A1 stores a digital certificate identifying the user, but does not explicitly describe storing security data used to access particular computing resources as described by security setup data. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20090036164-A1 | Status | Explanation |
|---|---|---|---|---|
| 3 | a **reader for automatically detecting the presence of the personal digital key** and **establishing a link with the personal digital key**, | **wirelessly communicatively coupling a portable device to a personal area network (PAN)** to **receive an authentication request from a computer**; (Claim 9) | Partial | US-20090036164-A1 discloses wireless coupling and authentication but does not explicitly describe a separate reader device detecting presence and establishing a link. |
| 4 | the reader having an input and an output and adapted for **wireless communication with the personal digital key** when the reader and the personal digital key are within the predefined range of each other, | **wireless transceiver to communicatively couple to a personal area network (PAN)** (Claim 1) | Partial | US-20090036164-A1 discloses wireless communication within a PAN but does not detail the reader's input/ output structure as in US-9251332-B2. |
| 5 | the reader **automatically signaling a computing device whether it is linked to the personal digital key**; | the wireless transceiver **sends** the encrypted message to the **computer** via the PAN (Claim 2) | Partial | US-20090036164-A1 discloses communication of messages to the computer but does not explicitly describe signaling link status as in US-9251332-B2. |
| 6 | the **computing device** having computing resources including the particular computing resource, | a **personal computer** communicatively coupled to the apparatus via the PAN, wherein the **personal computer** allows access by the user if the user is authenticated using the apparatus; (Claim 8) | Match | US-20090036164-A1 discloses a computing device with resources accessed upon authentication by the portable device. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20090036164-A1 | Status | Explanation |
|---|---|---|---|---|
| 7 | "the **computing device coupled to the input and the output of the reader** for **sending and receiving data**;" | "**wirelessly communicatively coupling a portable device** to a personal area network (PAN) to **receive an authentication request** from a computer; (Claim 9)" | Partial | US-20090036164-A1 discloses data exchange between portable device and computer but does not specify coupling via reader input/ output as in US-9251332-B2. |
| 8 | the computing device including **a security system for controlling access to the computing resources of the computing device** based on **security set up data**, | **authenticating the user in response to the authentication request** using the digital certificate, wherein the user is allowed to **access the device upon authentication**; (Claim 1) | Partial | US-20090036164-A1 discloses access control based on authentication but does not mention security setup data controlling access. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | the digital certificate is protected from being extracted by devices external to the apparatus; (Claim 7) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20090036164-A1 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | | Not Found | |
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | | Not Found | |
| 12 | the **security system controlled by the signal from the reader** indicating whether the **reader is linked to the personal digital key**, | the **wireless transceiver sends the encrypted message** to the computer via the **PAN** (Claim 2) | Partial | US-20090036164-A1 discloses communication of messages but does not explicitly describe control of security system by reader signals indicating link status. |
| 13 | and **terminating access to the computing resource** based on an **exit-based rule** of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | the user is automatically **logged off from the computer** if the wireless transceiver has been communicatively decoupled from the PAN for a **predetermined period**; (Claim 3) | Match | US-20090036164-A1 discloses automatic logoff when the portable device is decoupled from the PAN, similar to exit-based rule termination of access. |

**Rank 5:** EP-1271277-A2 **Priority Date:** 2001-06-26

**Assignee:** Redstrike B.V.

**Inventor(s):** Yaachov Behar

**Patent Reference:** https://patents.google.com/patent/EP1271277A2

## Similarity Analysis:

EP-1271277-A2 discloses a security system with a key device carrying key identification and a computing device with memory storing validation records, and an interface for exchanging key identification. It includes software to validate the key and inhibit use if validation fails. US-9251332-B2 describes a personal digital key with wireless communication within a predefined range, a reader detecting the key and signaling the computing device, and a security system controlling access based on security setup data stored encrypted in the computing device. EP-1271277-A2 captures the concept of a key device and validation but lacks explicit mention of wireless communication within a predefined range, a reader signaling link status, user-defined security actions including biometric confirmation, and exit-based rules for terminating access based on proximity. Thus, EP-1271277-A2 partially overlaps but does not fully capture all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

EP-1271277-A2 does not explicitly disclose all elements of Claim-1 of US-9251332-B2, particularly the wireless communication within a predefined range, the reader automatically signaling link status, the dedicated encrypted memory portion excluding security data but including user-defined options, biometric confirmation, and exit-based rules for terminating access when the key is out of range. These features are critical to US-9251332-B2's claim and are not inherently or expressly described in EP-1271277-A2. Therefore, EP-1271277-A2 does not anticipate US-9251332-B2 under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2 introduces novel elements such as a personal digital key adapted for wireless communication within a predefined range, a reader that automatically detects and signals link status, a security system using encrypted setup data excluding security data but including user-defined options for different security actions including biometric confirmation, and exit-based rules for terminating access. These features are not disclosed or suggested in EP-1271277-A2,

which focuses on key identification validation and access inhibition without these specific wireless and user-configurable security features. Hence, US-9251332-B2 is novel over EP-1271277-A2.

### Obviousness Analysis:

While EP-1271277-A2 discloses a key device and validation system, the extension to wireless communication within a predefined range, a reader signaling link status, encrypted security setup data with user-defined options including biometric confirmation, and exit-based rules for access termination could be considered non-obvious improvements. However, given the general knowledge in security systems, some aspects like wireless communication and access control might be obvious to a person skilled in the art. The biometric confirmation and exit-based rules might be less obvious. Therefore, obviousness is uncertain and requires further analysis.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in EP-1271277-A2 | Status | Explanation |
|---|---|---|---|---|
| 1 | "a **personal digital key adapted for wireless communication** within a predefined range to establish a link and send and receive data," | "A security system according to anyone of the preceding claims characterized in that said interface comprises **a wireless connection between the key device** and the computing device. (Claims) " | Partial | EP-1271277-A2 discloses wireless connection between key device and computing device but does not specify predefined range or link establishment details as in US-9251332-B2. |
| 2 | the **personal digital key associated with a user** and **storing security data used to access a particular computing resource** as described by **security set up data for the particular computing resource**; | The **key device** comprises programmable memory means to **store further key information**... enabling the computer program to automatically add a validation record associated with said key device and to grant privileges to the key device depending on the contents of said **further key information**. (Claims) | Partial | EP-1271277-A2 stores key information and grants privileges but does not explicitly describe storing security data specific to particular computing resources as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in EP-1271277-A2 | Status | Explanation |
|---|---|---|---|---|
| 3 | a **reader for automatically detecting the presence of the personal digital key** and **establishing a link with the personal digital key**, | An **interface to connect said key device** with said computing device and to provide a **pathway to exchange said key identification**; (Abstract) | Partial | EP-1271277-A2 discloses an interface connecting key device and computing device but does not explicitly describe a reader automatically detecting presence and establishing a link. |
| 4 | "the reader having an input and an output and adapted for **wireless communication with the personal digital key** when the reader and the personal digital key are within the predefined range of each other," | "Said interface comprises **a wireless connection between the key device and the computing device**. (Claims)" | Partial | EP-1271277-A2 mentions wireless interface but lacks details on input/ output structure and predefined range conditions. |
| 5 | "the reader **automatically signaling a computing device whether it is linked to the personal digital key**;" | "The computer program is capable of **accessing said further key information upon connection** of the key device with the **computing device**. (Claims)" | Partial | EP-1271277-A2 implies communication upon connection but does not explicitly describe automatic signaling of link status by the reader. |
| 6 | "the **computing device** having **computing resources** including the particular computing resource," | "A **computing device** with **memory means** installed for storing validation records and running software to validate key identification." | Match | EP-1271277-A2 discloses a computing device with resources and memory for validation, matching this element. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in EP-1271277-A2 | Status | Explanation |
|---|---|---|---|---|
| 7 | "the **computing device** coupled to the input and the output of the reader for **sending and receiving data**;" | "An interface to connect said key device with said **computing device** and to provide a pathway to **exchange said key identification**;" | Partial | EP-1271277-A2 discloses an interface for data exchange but does not detail coupling to input/output of a reader as in US-9251332-B2. |
| 8 | the computing device including **a security system for controlling access to the computing resources of the computing device based on security set up data**, | A program to **validate said key identification embedded in said key device using said validation record**; and means for inhibiting use of said computing device if said key identification and said validation record do not match. (Abstract) | Partial | EP-1271277-A2 includes a security program controlling access but does not specify use of security setup data as in US-9251332-B2. |
| 9 | wherein the **security set up data is stored in a dedicated encrypted portion of a memory of the computing device** and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | The **validation record is stored in memory means installed in the computing device**. (Abstract) | Partial | EP-1271277-A2 stores validation records but does not specify dedicated encrypted portion excluding security data as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in EP-1271277-A2 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the **security set up data** is based on one or more user defined options allowing the user to implement **different security actions for different computing resources**, | The computer program grants **privileges** to the key device depending on the contents of said **further key information**. (Claims) | Partial | EP-1271277-A2 grants privileges based on key information but does not describe user-defined options for different security actions per resource. |
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | | Not Found | |
| 12 | the **security system controlled by the signal from the reader** indicating whether the **reader is linked to the personal digital key**, | The **computer program accesses key information upon connection** of the **key device with the computing device**. (Claims) | Partial | EP-1271277-A2 implies control based on connection but does not explicitly describe control by signal from reader indicating link status. |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | | Not Found | |

**Rank 6:** US-20060176146-A1 **Priority Date:** 2005-02-09

**Assignee:** Baldev Krishan; Gurminder Singh

**Inventor(s):** Baldev Krishan

**Patent Reference:** https://patents.google.com/patent/US20060176146A1

## Similarity Analysis:

US-20060176146-A1 discloses a wireless USB memory key with fingerprint authentication used to control access to computing equipment wirelessly. US-9251332-B2 describes a system with a personal digital key for wireless communication within a predefined range, a reader detecting the key, and a computing device controlling access based on security setup data including biometric confirmation. Both involve wireless keys and biometric authentication. However, US-9251332-B2 emphasizes a dedicated encrypted memory portion with user-defined security actions and exit-based rules for access termination based on proximity, which are not explicitly described in US-20060176146-A1. US-20060176146-A1 focuses on fingerprint authentication and wireless control but lacks detailed description of security setup data, user-defined options, and exit-based rules. Thus, US-20060176146-A1 partially captures the ideas but may not fully encompass all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20060176146-A1 does not explicitly or inherently disclose all elements of Claim-1 of US-9251332-B2, particularly the dedicated encrypted portion of memory storing security setup data excluding security data, user-defined options for different security actions, and exit-based rules for terminating access when the key is out of range. While US-20060176146-A1 includes wireless communication and fingerprint authentication, it lacks the detailed security system architecture and control mechanisms described in US-9251332-B2. Therefore, US-20060176146-A1 does not anticipate US-9251332-B2 under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2 is novel over US-20060176146-A1 because it introduces a unique combination of features: a personal digital key with wireless communication within a predefined range, a reader signaling link status, a computing device with a dedicated encrypted memory portion storing security setup data (excluding security data), user-defined security actions including biometric confirmation, and exit-based rules for access termination. US-20060176146-A1, while disclosing wireless USB keys with fingerprint authentication, does not disclose the dedicated encrypted

security setup data, user-configurable security actions, or exit-based rules. Thus, US-9251332-B2's novel integration of these elements is not found in US-20060176146-A1.

### Obviousness Analysis:

Some elements of Claim-1 in US-9251332-B2, such as wireless communication and biometric authentication, are disclosed in US-20060176146-A1, suggesting these features are known. However, the dedicated encrypted memory portion with user-defined security actions and exit-based rules for access termination are not explicitly disclosed or suggested in US-20060176146-A1. It could be argued that implementing user-defined security actions and exit-based rules is an obvious extension to enhance security. Yet, without explicit or implicit teaching in US-20060176146-A1, the obviousness is uncertain. Therefore, the obviousness status is maybe.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060176146-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | "a **personal digital key adapted for wireless communication** within a predefined range to establish a link and send and receive data," | "A wireless universal serial bus (USB) memory key with fingerprint authentication, comprising: ... a **radio-frequency (RF) transceiver for supporting wireless communications**; ..." | Match | Direct correspondence in functionality as both describe a wireless key capable of communication within a range. |
| 2 | "the **personal digital key associated with a user** and **storing security data used to access a particular computing resource** as described by security set up data for the particular computing resource;" | "The **USB memory key** contains memory for **storing data files and user fingerprints for authentication**. (Abstract, Claim 13)" | Partial | US-20060176146-A1 stores user data and fingerprints but does not explicitly describe storing security data used to access particular computing resources as per security setup data. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060176146-A1 | Status | Explanation |
|---|---|---|---|---|
| 3 | a **reader for automatically detecting the presence of the personal digital key** and establishing a link with the personal digital key, | The **wireless USB memory key forms a wireless communications link** with computing equipment. (Claim 19) | Partial | US-20060176146-A1 describes wireless link establishment but does not explicitly describe a separate reader device detecting the key. |
| 4 | "the reader having an input and an output and adapted for **wireless communication** with the personal digital key when the reader and the personal digital key are within the predefined range of each other," | "The USB memory key includes **an RF transceiver for wireless communication**. (Claim 13)" | Partial | US-20060176146-A1 discloses wireless communication but does not detail reader input/output structure as in US-9251332-B2. |
| 5 | the reader **automatically signaling a computing device whether it is linked to the personal digital key**; | The wireless USB memory key **wirelessly controls computing equipment upon successful authentication**. (Claims 1, 4) | Partial | US-20060176146-A1 implies signaling via control but does not explicitly describe the reader signaling link status to computing device. |
| 6 | the **computing device** having **computing resources** including the particular computing resource, | The **computing equipment** controlled by the wireless USB memory key includes **computer networks and other equipment**. (Claims 4, 5) | Match | US-20060176146-A1 discloses computing equipment with resources controlled by the key. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060176146-A1 | Status | Explanation |
|---|---|---|---|---|
| 7 | "the **computing device** coupled to the input and the output of the reader for sending and receiving data;" | "The wireless USB memory key communicates wirelessly with **computing equipment**. (Claims 1, 13)" | Partial | US-20060176146-A1 discloses wireless communication but does not explicitly describe coupling via reader input/ output as in US-9251332-B2. |
| 8 | the computing device including **a security system for controlling access to the computing resources of the computing device** based on security set up data, | The system uses **fingerprint authentication to control access to computing equipment**. (Claims 1, 9, 10) | Partial | US-20060176146-A1 includes authentication but lacks detailed security system based on security setup data as in US-9251332-B2. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | Not found | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060176146-A1 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | Not found | Not Found | |
| 11 | wherein the different security actions include a **biometric confirmation** for a respective computing resource, | The USB memory key includes a **fingerprint sensor for biometric authentication**. (Claims 1, 13) | Match | Direct match on biometric confirmation via fingerprint sensor. |
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key, | Not found | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | Not found | Not Found | |

**Rank 7:** US-20080267404-A1 **Priority Date:** 2002-07-29

**Assignee:** Wolfgang Otto Budde; Oliver Schreyer; Armand Lelkens; Bozena Erdmann

**Inventor(s):** Wolfgang Otto Budde

**Patent Reference:** https://patents.google.com/patent/US20080267404A1

## Similarity Analysis:

US-20080267404-A1 discloses a security system for wireless networks with a portable unit storing a key record for short-range transmission and a receiving unit in a wireless apparatus that processes the key record. US-9251332-B2 describes a system with a personal digital key for wireless communication within a predefined range, a reader detecting the key and signaling a computing device, and a security system controlling access based on security setup data excluding the security data itself. Both involve wireless short-range communication for security access control and include biometric elements. However, US-20080267404-A1 focuses on key records for network authentication and encryption, while US-9251332-B2 emphasizes user-defined security actions, encrypted setup data, and exit-based rules for access termination. The concepts overlap in wireless security and biometric use but differ in system architecture and specific control mechanisms, making the similarity partial and inconclusive for full capture of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20080267404-A1 does not explicitly or inherently disclose all elements of Claim-1 of US-9251332-B2, particularly the dedicated encrypted portion of memory storing security setup data excluding the security data, user-defined options for different security actions per resource, biometric confirmation as a security action, and exit-based rules for terminating access when the key is out of range. US-20080267404-A1 focuses on key record transmission and network authentication/encryption but lacks detailed disclosure of controlling access to computing resources with user-configurable security actions and exit-based rules. Therefore, US-20080267404-A1 does not anticipate US-9251332-B2 under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2 introduces novel elements such as a personal digital key linked wirelessly within a predefined range, a dedicated encrypted memory portion storing security setup data excluding the security data, user-defined security actions including biometric confirmation, and exit-based rules for terminating access. US-20080267404-A1, while related to wireless security and biometric

key records, does not disclose these specific features or the detailed control mechanisms of access termination and user-configurable security actions. Thus, US-9251332-B2 retains novelty over US-20080267404-A1.

### Obviousness Analysis:

Some elements of Claim-1 in US-9251332-B2, such as wireless communication of a security key and biometric authentication, are conceptually related to US-20080267404-A1. However, the specific implementation of a dedicated encrypted memory portion for security setup data excluding the security data, user-defined security actions per resource, and exit-based rules for access termination are not explicitly or inherently disclosed in US-20080267404-A1. These could be considered non-obvious extensions or combinations of known wireless security concepts. Therefore, obviousness is uncertain without further evidence or expert testimony.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080267404-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | **a personal digital key** adapted for **wireless communication within a predefined range** to establish a link and send and receive data, | **a first portable unit (1) with a memory (3) for storing a worldwide unambiguous key record (4)** provided for **short-range information transmission** of the key record (4) (Claim 1) | Match | Both disclose a portable unit/key adapted for short-range wireless communication to transmit security data. |
| 2 | "the **personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by security set up data for the particular computing resource;" | "the portable unit (1) comprises an input device (50) for providing **a key record** to the memory (3) and can derive **a key record from biometric characteristics of a user** (Claim 3, 4)" | Partial | US-20080267404-A1 associates the key record with user biometric data but does not explicitly describe storing security data for accessing particular computing resources as per US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080267404-A1 | Status | Explanation |
|---|---|---|---|---|
| 3 | a **reader for automatically detecting the presence of the personal digital key** and establishing a link with the personal digital key, | at least one **receiving unit (7) in at least one wireless apparatus (2) of the network, comprising a receiver (9) for receiving the key record (4)** (Claim 1) | Match | US-20080267404-A1 discloses a receiving unit that detects and receives the key record from the portable unit, analogous to the reader detecting the personal digital key. |
| 4 | "the **reader** having **an input and an output** and adapted for **wireless communication** with the personal digital key when the reader and the personal digital key are within the predefined range of each other," | "the **receiving unit (7)** comprising **a receiver (9)** for **receiving the key record (4)** and an evaluation component (11) for processing the key record (Claim 1)" | Partial | US-20080267404-A1 describes wireless communication and processing but does not explicitly mention input/ output ports or signaling to a computing device as in US-9251332-B2. |
| 5 | the **reader automatically signaling a computing device** whether it is **linked to the personal digital key**; | the **evaluation component (11) of the apparatus for storing, processing and/or passing on** the key record (4) or a part of the key record to a second component (Claim 1) **linked to the personal digital key** | Partial | US-20080267404-A1 includes passing on the key record to another component, which may correspond to signaling, but lacks explicit automatic signaling of link status to a computing device. |
| 6 | the **computing device** having computing resources including the particular computing resource, | the **wireless apparatus (2)** of the network (Claim 1) | Partial | US-20080267404-A1 mentions a wireless apparatus but does not detail computing resources or particular computing resources as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080267404-A1 | Status | Explanation |
|---|---|---|---|---|
| 7 | the **computing device** coupled to the input and the output of the reader for **sending and receiving data**; | the **apparatus (2)** for **storing, processing and/or passing on** the key record (Claim 1) | Partial | US-20080267404-A1 discloses data processing and passing but does not explicitly describe coupling to input/output of a reader for data exchange as in US-9251332-B2. |
| 8 | the computing device including a **security system for controlling access to the computing resources of the computing device** based on **security set up data**, | the apparatus (2) is provided for **authentication and encryption of useful data to be transmitted between the apparatuses of the network** by means of a **key comprised in the key record** (Claim 15) | Partial | US-20080267404-A1 includes authentication and encryption using the key record but does not disclose controlling access to computing resources based on security setup data as in US-9251332-B2. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | Not found | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080267404-A1 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | Not found | Not Found | |
| 11 | wherein the different security actions include a **biometric confirmation** for a respective computing resource, | the portable unit (1) can derive a **key record from biometric characteristics** of a user (Claim 4) | Partial | US-20080267404-A1 includes biometric characteristics for key record derivation but does not specify biometric confirmation as a security action per computing resource. |
| 12 | the **security system controlled by the signal from the reader** indicating whether the reader is linked to the **personal digital key**, | the **evaluation component (11) for processing and/or passing on** the **key record** (Claim 1) | Partial | US-20080267404-A1 processes the key record but does not explicitly disclose control of the security system by a signal indicating link status. |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | Not found | Not Found | |

**Rank 8:** US-20080046751-A1 **Priority Date:** 2006-08-14

**Assignee:** Advanced Digital Chips Inc.

**Inventor(s):** In Chul Choi

**Patent Reference:** https://patents.google.com/patent/US20080046751A1

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, including user-defined security actions like biometric confirmation and exit-based rules for terminating access when the PDK is out of range. US-20080046751-A1 discloses a USB device-based security system that installs a security program on a local computer, uses USB connection for authentication, and includes fingerprint authentication. However, US-20080046751-A1 lacks the wireless communication within a predefined range, the concept of a reader signaling the computing device about the link status, and the exit-based rule for terminating access based on proximity. US-20080046751-A1 focuses on USB connection and automatic program installation rather than wireless proximity-based access control. Thus, US-20080046751-A1 does not capture all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20080046751-A1 does not anticipate US-9251332-B2 because it does not disclose or inherently describe the wireless communication within a predefined range between a personal digital key and a reader, nor the security setup data stored in a dedicated encrypted portion of memory excluding the security data itself. The exit-based rule for terminating access when the key is out of range is also absent. US-20080046751-A1's USB-based authentication and security program installation differ fundamentally from the wireless proximity-based security system of US-9251332-B2. Therefore, US-20080046751-A1 does not anticipate the claimed invention of US-9251332-B2 under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2 is novel over US-20080046751-A1 because it introduces a unique wireless personal digital key system with proximity-based access control, dedicated encrypted security setup data excluding the security data, and user-configurable security actions including biometric confirmation and exit-based access termination. US-20080046751-A1's USB device-based security

system does not disclose these features, particularly the wireless communication and exit-based rules. Hence, the novelty of US-9251332-B2 is not invalidated by US-20080046751-A1.

### Obviousness Analysis:

The elements of Claim-1 in US-9251332-B2 are not obvious extensions of US-20080046751-A1. US-20080046751-A1 focuses on USB device-based security with automatic program installation and fingerprint authentication but does not suggest wireless communication within a predefined range, nor the use of a reader signaling the computing device or exit-based rules for access termination. The differences in communication method and security control approach are significant, making the claimed invention non-obvious over US-20080046751-A1 under 35 U.S.C. §103.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080046751-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | "a **personal digital key adapted for wireless communication within a predefined range** to establish a link and send and receive data," | "The USB device includes an **RF module to perform authentication through RF communication**, the RF module being used for an admission ticket of a building." | Partial | US-20080046751-A1 discloses an RF module for authentication, which is a form of wireless communication, but it is not described as a personal digital key adapted for wireless communication within a predefined range to establish a link and send and receive data as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080046751-A1 | Status | Explanation |
|---|---|---|---|---|
| 2 | "the **personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by security set up data for the particular computing resource;" | "The USB device stores **authentication information** including **fingerprint data used for user authentication**. (Claims 4, 5, 14, 15)" | Partial | US-20080046751-A1 stores authentication data in the USB device but does not describe storing security data used to access particular computing resources as described by security setup data in US-9251332-B2. |
| 3 | "a **reader for automatically detecting the presence of the personal digital key** and **establishing a link with the personal digital key**," | "The USB device connects to the local computer via **USB communication means** and the security program **authenticates the USB device**. (Claims 1, 4)" | Partial | US-20080046751-A1's USB device connects to the computer and is authenticated, but there is no separate reader device that automatically detects presence and establishes a wireless link as in US-9251332-B2. |
| 4 | "the reader having an input and an output and adapted for **wireless communication** with the personal digital key when the reader and the personal digital key are within the predefined range of each other," | "The USB device includes **an RF module for authentication via RF communication**. (Claims 10, 20)" | Partial | US-20080046751-A1 includes an RF module for wireless communication, but the reader's input/ output and wireless communication within a predefined range as a separate device is not disclosed. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080046751-A1 | Status | Explanation |
|---|---|---|---|---|
| 5 | the reader **automatically signaling a computing device whether it is linked to the personal digital key**; | The security program installed on the local computer **authenticates the USB device** and **controls access accordingly**. (Claims 1, 4) | Partial | US-20080046751-A1's security program authenticates the USB device but does not describe the reader signaling the computing device about the link status as a separate function. |
| 6 | the **computing device** having **computing resources** including the particular computing resource, | The local **computer** has various application programs and **computing resources**. (Abstract, Claims 1) | Match | US-20080046751-A1 discloses a local computer with application programs and computing resources, matching this element. |
| 7 | "the **computing device coupled to the input and the output of the reader** for sending and receiving data;" | "The **USB device connects to the local computer via USB communication means**. (Claims 1, 11)" | Match | US-20080046751-A1 discloses the USB device connected to the local computer for data communication, matching this element. |
| 8 | the computing device including **a security system for controlling access to the computing resources of the computing device** based on **security set up data**, | The **security program installed in the local computer controls access to files and resources** based on **authentication data from the USB device**. (Claims 1, 4, 7) | Partial | US-20080046751-A1 controls access based on authentication but does not describe security setup data stored in a dedicated encrypted portion excluding the security data itself. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080046751-A1 | Status | Explanation |
|---|---|---|---|---|
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | Not found | Not Found | |
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | Not found | Not Found | |
| 11 | wherein the different security actions include a **biometric confirmation** for a respective computing resource, | The USB device includes **fingerprint authentication** means for user authentication. (Claims 5, 15) | Partial | US-20080046751-A1 includes biometric (fingerprint) authentication but does not specify it per computing resource as a user-defined security action. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080046751-A1 | Status | Explanation |
|---|---|---|---|---|
| 12 | "the **security system controlled by the signal from the reader** indicating whether the reader is linked to the personal digital key," | "The **security program controls access based on authentication of the USB device**. (Claims 1, 4)" | Partial | US-20080046751-A1 controls access based on USB device authentication but does not describe control based on a reader's signal indicating link status. |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | Not found | Not Found | |

**Rank 9:** US-20080098468-A1 **Priority Date:** 2000-06-24

**Assignee:** Palm; Inc.

**Inventor(s):** Michael Cortopassi

**Patent Reference:** https://patents.google.com/patent/US20080098468A1

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, with a reader detecting the PDK and a computing device controlling access based on encrypted security setup data including biometric options and exit-based rules. US-20080098468-A1 discloses a system where a first device (e.g., PDA) wirelessly sends a password to a second device when in proximity, which then grants or denies access based on the password. Both involve wireless communication for access control using a personal device and a computing device. However, US-20080098468-A1 lacks explicit mention of encrypted security setup data, user-defined security actions, biometric confirmation, or exit-based rules for terminating access when out of range. Thus, US-20080098468-A1 captures some core ideas but not all detailed aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20080098468-A1 anticipates the general concept of wireless proximity-based access control using a personal device transmitting a password to a computing device. However, it does not explicitly or inherently disclose the dedicated encrypted portion of memory storing security setup data excluding the security data, user-defined options for different security actions, biometric confirmation, or exit-based rules for terminating access when the personal digital key is out of range. These features are critical elements of Claim-1 in US-9251332-B2 and are not found in US-20080098468-A1, so US-20080098468-A1 does not fully anticipate US-9251332-B2.

## Novelty Analysis:

US-9251332-B2 is novel over US-20080098468-A1 because it introduces unique features not disclosed in US-20080098468-A1, including the use of a dedicated encrypted memory portion storing security setup data separate from the security data, user-configurable security actions for different computing resources, biometric confirmation as a security action, and automatic termination of access based on exit-based rules when the personal digital key is no longer within

range. These novel elements distinguish US-9251332-B2 from the simpler proximity-based password transmission system of US-20080098468-A1.

### Obviousness Analysis:

While US-20080098468-A1 discloses wireless proximity-based access control using a personal device transmitting a password, the additional features in US-9251332-B2 such as encrypted security setup data, user-defined security actions including biometrics, and exit-based rules for terminating access could be considered obvious extensions to someone skilled in the art seeking to improve security. However, the specific combination and implementation details may not be straightforward or suggested explicitly in US-20080098468-A1, so obviousness is uncertain without further evidence.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080098468-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a **personal digital key adapted for wireless communication within a predefined range** to establish a link and **send and receive data**, | a **first computing device that outputs a signal containing a password automatically in response to being located in proximity to a second computing device**... said first computing device **communicates with said second computing device wirelessly** (Claims 1, 13) | Match | Strong match as both disclose a personal device wirelessly communicating within a predefined range to establish a link and send data (password). |
| 2 | the **personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by security set up data for the particular computing resource; | said first computing device comprises a memory device that stores **said password** (Claim 10) and **said password is unique to a given person** (Claim 8) | Partial | US-20080098468-A1 stores security data (password) associated with a user, but does not describe security setup data for particular computing resources as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080098468-A1 | Status | Explanation |
|---|---|---|---|---|
| 3 | a **reader for automatically detecting the presence of the personal digital key** and **establishing a link with the personal digital key**, | the second computing device **receives said password** and **determines if it is authorized** (Claim 1) | Partial | US-20080098468-A1's second device detects the presence of the first device via password reception but does not explicitly describe a separate reader device automatically detecting presence and establishing a link. |
| 4 | the reader having an input and an output and adapted for **wireless communication** with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | said first computing device **communicates ... wirelessly** with said second computing device (Claim 13) | Partial | Wireless communication between devices is disclosed, but the reader's input/ output structure is not explicitly described. |
| 5 | the reader **automatically signaling a computing device whether it is linked to the personal digital key**; | the second computing device **determines if the password is authorized** and permits or denies access (Claim 1) | Partial | US-20080098468-A1 discloses signaling access permission based on password but does not explicitly describe the reader signaling link status to the computing device. |
| 6 | the **computing device** having computing resources including the particular computing resource, | the **second computing device** permits access to a secure area if password is authorized (Claim 1) | Match | Strong match as both describe a computing device controlling access to computing resources based on received credentials. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080098468-A1 | Status | Explanation |
|---|---|---|---|---|
| 7 | "the **computing device** coupled to the input and the output of the reader for **sending and receiving data**;" | "**computing devices** (Claim 13) **wireless communication** between first and second **computing devices**" | Partial | US-20080098468-A1 discloses wireless communication but does not explicitly describe coupling via input/output ports as a reader device. |
| 8 | the computing device including **a security system for controlling access to the computing resources of the computing device based on security set up data**, | the second computing device **determines if the password is authorized and permits or denies access** (Claim 1) | Partial | US-20080098468-A1 controls access based on password but does not disclose security setup data controlling access. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20080098468-A1 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | | Not Found | |
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | | Not Found | |
| 12 | the **security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key**, | the **second computing device determines if the password is authorized and permits or denies access** (Claim 1) | Partial | US-20080098468-A1 controls access based on password reception but does not explicitly describe control by reader signal indicating link status. |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | | Not Found | |

**Rank 10:** US-20220217138-A1 **Priority Date:** 2004-03-08

**Assignee:** Proxense; Llc

**Inventor(s):** John J. Giobbi

**Patent Reference:** https://patents.google.com/patent/US20220217138A1

## Similarity Analysis:

US-9251332-B2 describes a security system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, including biometric confirmation and exit-based rules for terminating access. US-20220217138-A1 also involves a personal digital key and a computing device with a reader/decoder circuit that wirelessly receives an activation code from the PDK and authenticates it to provide access to digital content. Both patents involve wireless communication with a PDK and controlling access based on authentication. However, US-20220217138-A1 focuses on digital content access and authentication via a key provider, lacking explicit mention of biometric confirmation, exit-based rules, or dedicated encrypted memory storing security setup data as in US-9251332-B2. Thus, US-20220217138-A1 captures some but not all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20220217138-A1 does not explicitly disclose or inherently describe all elements of Claim-1 of US-9251332-B2, particularly the dedicated encrypted portion of memory storing security setup data excluding security data, user-defined options for different security actions including biometric confirmation, and exit-based rules terminating access when the PDK is out of range. The focus of US-20220217138-A1 is on authentication of a PDK to access digital content, not on comprehensive security system controlling multiple computing resources with user-configurable security actions. Therefore, US-20220217138-A1 does not anticipate US-9251332-B2.

## Novelty Analysis:

US-9251332-B2 is novel over US-20220217138-A1 because it introduces a unique combination of features: a personal digital key communicating wirelessly within a predefined range, a reader signaling link status, a computing device with a security system controlling access based on security setup data stored in a dedicated encrypted memory portion (excluding security data), user-defined security actions including biometric confirmation, and exit-based rules for terminating access. US-20220217138-A1 lacks these specific features and focuses on authentication for digital content access, thus not invalidating the novelty of US-9251332-B2.

**Obviousness Analysis:**

While US-20220217138-A1 discloses wireless communication with a personal digital key and authentication to control access, it does not explicitly or inherently suggest the dedicated encrypted memory storing security setup data excluding security data, user-defined security actions including biometrics, or exit-based rules for terminating access. These features could be considered non-obvious extensions. However, given the shared concept of PDK-based access control, a skilled person might find it obvious to extend US-20220217138-A1's system to include some of these features. Therefore, obviousness is uncertain without further evidence.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20220217138-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | **a personal digital key** adapted for **wireless communication** within a predefined range to establish a link and **send and receive data**, | **a tangible personal digital key** including a first activation code comprising a user label and an account number and a first **wireless transceiver** to **wirelessly transmit** the first activation code; | Match | Both patents disclose a personal digital key with wireless communication capabilities to establish a link and transmit data. |
| 2 | the **personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by security set up data for the particular computing resource; | the first activation code comprising **a user label** and **an account number**; | Partial | US-20220217138-A1's PDK stores user label and account number for authentication, but does not explicitly disclose storing security data for accessing particular computing resources as described by security setup data. |
| 3 | a **reader** for automatically **detecting the presence of the personal digital key** and establishing a link with the personal digital key, | a computing device comprising a **reader**/decoder circuit that **receives the first activation code from the tangible personal digital key**; | Match | US-20220217138-A1 discloses a reader/ decoder circuit that automatically receives data from the PDK, establishing a link. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20220217138-A1 | Status | Explanation |
|---|---|---|---|---|
| 4 | the reader having **an input and an output** and **adapted for wireless communication** with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | the first **wireless** transceiver to **wirelessly transmit** the first activation code; | Partial | US-20220217138-A1 discloses wireless communication between PDK and reader, but does not explicitly mention input/output structure or predefined range. |
| 5 | the reader **automatically signaling a computing device whether it is linked to the personal digital key**; | the **computing device** transmits the first activation code received from the **PDK** to a key provider device for authentication; | Partial | US-20220217138-A1 involves signaling for authentication but does not explicitly disclose the reader signaling the computing device about link status. |
| 6 | the **computing device** having computing resources including the particular computing resource, | a **computing device** coupled to the tangible personal digital key via a wireless network; | Partial | US-20220217138-A1 discloses a computing device coupled to the PDK, but does not detail computing resources or particular resources as in US-9251332-B2. |
| 7 | "the **computing device** coupled to the input and the output of the reader for **sending and receiving data**;" | "the **computing device** **receives** the first activation code from the PDK and **transmits** it to a key provider device;" | Partial | US-20220217138-A1 discloses data transmission between computing device and PDK via reader, but lacks explicit input/output coupling details. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20220217138-A1 | Status | Explanation |
|---|---|---|---|---|
| 8 | the **computing device** including a **security system for controlling access** to the **computing resources of the computing device** based on security set up data, | the **computing device** is programmed to receive digital content marked with an unlock code associated with the first activation code from a content provider device responsive to **authentication**; | Partial | US-20220217138-A1 controls access to digital content based on authentication but does not disclose a security system controlling access based on security setup data. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | | Not Found | |
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | | Not Found | |
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20220217138-A1 | Status | Explanation |
|---|---|---|---|---|
| 12 | the security system controlled by the **signal from the reader indicating whether the reader is linked to the personal digital key**, | the computing device receives the **first activation code from the PDK and authenticates it**; | Partial | US-20220217138-A1 involves authentication signaling but does not explicitly disclose control of security system by reader signal indicating link status. |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | | Not Found | |

**Rank 11:** US-20040059919-A1 **Priority Date:** 2001-01-11

**Assignee:** Alain Benayoun; Jacques Fieschi; Jean-Francois Le Pennec; Pascal Roy

**Inventor(s):** Alain Benayoun

**Patent Reference:** https://patents.google.com/patent/US20040059919A1

### Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, including user-defined security actions like biometric confirmation and exit-based rules for terminating access when the PDK is out of range. US-20040059919-A1 focuses on an extractable security piece with a public key infrastructure (PKI) for mutual authentication with a PC security area, primarily using cryptographic keys and physical insertion/removal for access control. US-20040059919-A1 lacks the wireless communication within a predefined range, user-defined security actions, biometric confirmation, and exit-based rules as described in US-9251332-B2. Therefore, US-20040059919-A1 does not capture all aspects and ideas of Claim-1 in US-9251332-B2.

### Anticipation Analysis:

US-20040059919-A1 does not anticipate US-9251332-B2 because it does not disclose a personal digital key adapted for wireless communication within a predefined range, nor does it disclose user-defined security actions including biometric confirmation or exit-based rules for terminating access based on proximity. The mutual authentication via PKI in US-20040059919-A1 is different from the wireless proximity-based access control in US-9251332-B2. Thus, the elements of Claim-1 in US-9251332-B2 are not found, either expressly or inherently, in US-20040059919-A1.

### Novelty Analysis:

US-9251332-B2 is novel compared to US-20040059919-A1 because it introduces a unique combination of wireless personal digital key communication within a predefined range, dedicated encrypted security setup data excluding the security data itself, user-configurable security actions including biometric confirmation, and automatic termination of access based on proximity. US-20040059919-A1's focus on PKI-based mutual authentication with an extractable security piece does not disclose or suggest these features. Therefore, US-9251332-B2's novelty is not invalidated by US-20040059919-A1.

### Obviousness Analysis:

The elements of Claim-1 in US-9251332-B2 are not obvious extensions of the ideas in US-20040059919-A1. US-20040059919-A1's PKI-based authentication with an extractable security piece is fundamentally different from the wireless proximity-based system with user-defined security actions and biometric confirmation in US-9251332-B2. There is no teaching or suggestion in US-20040059919-A1 that would lead a person skilled in the art to combine or modify its system to arrive at the claimed invention in US-9251332-B2. Hence, the claim elements are not obvious over US-20040059919-A1.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20040059919-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a personal digital key adapted for wireless communication within a predefined range to establish a link and send and receive data, | An extractable security piece which can be removed from the main computer device by the authorized user, wherein the extractable security piece includes an extractable main private key and a main PC public key; (Claim 1) | Not Found | |
| 2 | "the **personal digital key associated with a user** and storing security data used to access a particular computing resource as described by security set up data for the particular computing resource;" | "The extractable security piece includes an **extractable main private key** and a main PC public key; (Claim 1)" | Partial | US-20040059919-A1's extractable security piece stores cryptographic keys but does not describe storing security data as described by security setup data for particular computing resources. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20040059919-A1 | Status | Explanation |
|---|---|---|---|---|
| 3 | a **reader for automatically detecting the presence of the personal digital key** and **establishing a link with the personal digital key**, | **Processing means in said extractable security piece and in said PC security area for mutual authentication of said extractable security piece and said PC security area** after said extractable security piece, which had been previously removed from said PC security area, is reinserted in said PC security area to **enable the authorized user to access data stored in said computer device**. (Claim 1) | Partial | US-20040059919-A1 discloses mutual authentication upon reinsertion of the security piece but does not disclose automatic detection or wireless link establishment within a predefined range. |
| 4 | the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | The extractable security piece includes a keyboard key of said computer device. (Claim 4) | Not Found | |
| 5 | the reader **automatically signaling a computing device whether it is linked to the personal digital key**; | **PKI checker for encrypting and authenticating data exchanged between said PC security area and said extractable security piece when said extractable security piece is reinserted in said main computer device**. (Claim 2) | Partial | US-20040059919-A1 discloses encrypted data exchange upon reinsertion but not automatic signaling of link status as in US-9251332-B2. |
| 6 | the **computing device** having computing resources including the particular computing resource, | **Main computer device** having an authorized user. (Claim 1) | Partial | US-20040059919-A1 discloses a main computer device but does not detail computing resources as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20040059919-A1 | Status | Explanation |
|---|---|---|---|---|
| 7 | "the **computing device** coupled to the input and the output of the reader for sending and receiving data;" | "The extractable security piece can be removed and reinserted into the **main computer device**. (Claim 1)" | Partial | US-20040059919-A1 discloses physical coupling but not wireless coupling for sending and receiving data as in US-9251332-B2. |
| 8 | the computing device including **a security system** for controlling access to the computing resources of the computing device based on security set up data, | **Security system** for preventing unauthorized use of a main computer device. (Title) | Partial | US-20040059919-A1 discloses a security system for preventing unauthorized use but does not specify control based on security setup data as in US-9251332-B2. |
| 9 | wherein the **security set up data is stored in a dedicated encrypted portion of a memory of the computing device** and includes **information on how to control access to the computing resources using security data**, but does not include the security data used to obtain access, | **PC security area, which is a non-extractable part of said computer device**, includes a **PC private key and an extractable main public key**. (Claim 1) | Partial | US-20040059919-A1 discloses a PC security area but does not describe dedicated encrypted memory storing security setup data excluding security data used for access. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20040059919-A1 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | | Not Found | |
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | | Not Found | |
| 12 | the **security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key**, | **Mutual authentication of said extractable security piece and said PC security area** after reinsertion. (Claim 1) | Partial | US-20040059919-A1 discloses mutual authentication after reinsertion but not control by a signal indicating link status as in US-9251332-B2. |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | | Not Found | |

**Rank 12:** US-9813416-B2 **Priority Date:** 2007-09-27

**Assignee:** Clevx; Llc

**Inventor(s):** Lev M. Bolotin

**Patent Reference:** https://patents.google.com/patent/US9813416B2

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, including user-defined security actions like biometric confirmation and exit-based rules for terminating access when the PDK is out of range. US-9813416-B2 focuses on a data security system with an electronic authentication subsystem verifying user identification against an authentication key, employing encryption keys, and wireless communication modules. However, US-9813416-B2 lacks the concept of a personal digital key linked to a reader that signals a computing device, user-configurable security actions per resource, and exit-based rules for access termination based on proximity. Thus, US-9813416-B2 does not capture all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-9813416-B2 does not explicitly or inherently disclose a personal digital key adapted for wireless communication within a predefined range linked to a reader that signals a computing device to control access based on user-defined security setup data including biometric confirmation and exit-based rules. The authentication and encryption focus in US-9813416-B2 is different from the proximity-based access control and user-configurable security actions in US-9251332-B2. Therefore, US-9813416-B2 does not anticipate US-9251332-B2.

## Novelty Analysis:

US-9251332-B2 introduces a unique integration of a personal digital key wirelessly linked to a reader that signals a computing device to control access based on encrypted security setup data with user-defined options including biometric confirmation and exit-based rules. US-9813416-B2, while addressing authentication and encryption, does not disclose these specific features or the proximity-based access control mechanism. Hence, US-9251332-B2 remains novel over US-9813416-B2.

## Obviousness Analysis:

The elements of Claim-1 in US-9251332-B2, such as the personal digital key with wireless communication within a predefined range, reader signaling, user-defined security actions including biometrics, and exit-based rules for terminating access, are not obvious extensions of the authentication and encryption methods described in US-9813416-B2. US-9813416-B2 does not suggest or motivate these specific features or their combination, so the claim elements are not obvious in view of US-9813416-B2.

### Additional Prior Art from the Same Patent Family:

Apart from US-9813416-B2 whose claim chart is provided below, US-9262611-B2 also belong to the same patent family. These may also aid in the invalidation of the subject patent. These patents disclose similar technical features and concepts that are relevant to the claims of the subject patent, potentially impacting its novelty and inventive step.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-9813416-B2 | Status | Explanation |
|---|---|---|---|---|
| 1 | a **personal digital key adapted for wireless communication** within a predefined range to establish a link and send and receive data | the electronic authentication subsystem includes a **wireless communication module** coupled to an authentication controller (Claim 9) | Partial | US-9813416-B2 discloses wireless communication in an authentication subsystem but does not describe a personal digital key adapted for proximity-based linking and data exchange as in US-9251332-B2. |
| 2 | the **personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by **security set up data for the particular computing resource** | **verifying a user identification** against an **authentication key**, the user identification supplied from outside a data security system to a receiver within an **electronic authentication subsystem** (Claim 1) | Partial | US-9813416-B2 verifies user identification against an authentication key but does not disclose storing security data specific to particular computing resources as described in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-9813416-B2 | Status | Explanation |
|---|---|---|---|---|
| 3 | "a **reader for automatically detecting the presence** of the personal digital key and establishing a link with the personal digital key" | "**wireless communication module including a radio frequency transmitter and a radio frequency receiver** (Claim 11)" | Partial | US-9813416-B2 discloses wireless communication modules but does not describe a reader device that automatically detects and links to a personal digital key. |
| 4 | the reader having **an input and an output** and adapted for **wireless communication** with the personal digital key when the reader and the personal digital key are within the predefined range of each other | **wireless communication** module includes **a radio frequency transmitter and a radio frequency receiver** for receiving the user identification (Claim 15) | Partial | US-9813416-B2 describes wireless communication but lacks the concept of a reader with input/ output adapted for proximity-based communication with a personal digital key. |
| 5 | the reader automatically signaling a computing device whether it is linked to the personal digital key | | Not Found | |
| 6 | the **computing device** having computing resources including the particular computing resource | **host computer system** (Claim 9) | Partial | US-9813416-B2 mentions a host computer system but does not detail computing resources as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-9813416-B2 | Status | Explanation |
|---|---|---|---|---|
| 7 | the computing device coupled to the input and the output of the reader for sending and receiving data | | Not Found | |
| 8 | the computing device including **a security system for controlling access to the computing resources of the computing device based on security set up data** | **data security system comprising an electronic authentication subsystem for verifying user identification and employing encryption keys** (Claim 9) | Partial | US-9813416-B2 includes a security system for authentication and encryption but lacks user-configurable security setup data controlling access to computing resources. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access | | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-9813416-B2 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources | | Not Found | |
| 11 | wherein the different security actions include a **biometric confirmation** for a respective computing resource | electronic authentication subsystem further includes a **biometric sensor** or an electro-mechanical input mechanism for receiving the user identification (Claim 12) | Partial | US-9813416-B2 discloses biometric sensors for user identification but not as part of user-defined security actions per resource. |
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key | | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range | | Not Found | |

**Rank 13:** US-20020042882-A1 **Priority Date:** 2000-10-10

**Assignee:** Dervan R. Donald; Taylor Richard Allyn

**Inventor(s):** R. Dervan

**Patent Reference:** https://patents.google.com/patent/US20020042882A1

### Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to establish a link with a reader, which signals a computing device to control access based on security setup data stored in encrypted memory. It includes user-defined security actions like biometric confirmation and exit-based rules to terminate access when the PDK is out of range. US-20020042882-A1 describes a computer security system with a terminal security access device that controls access using passwords, biometrics, and encrypted data transfer but does not disclose a wireless personal digital key, a reader establishing a link within a predefined range, or exit-based rules tied to proximity. Thus, US-20020042882-A1 lacks the specific wireless key-reader linkage and proximity-based access termination central to US-9251332-B2.

### Anticipation Analysis:

US-20020042882-A1 does not explicitly or inherently disclose a personal digital key adapted for wireless communication within a predefined range to establish a link with a reader that signals a computing device to control access. The absence of a wireless key-reader system and exit-based rules based on proximity means US-20020042882-A1 does not anticipate the claimed invention of US-9251332-B2 under 35 U.S.C. §102.

### Novelty Analysis:

US-9251332-B2's novelty lies in the integration of a wireless personal digital key and reader system that controls access based on encrypted security setup data with user-configurable security actions including biometric confirmation and exit-based rules triggered by proximity. US-20020042882-A1 lacks this wireless key-reader mechanism and proximity-based access control, thus US-9251332-B2 remains novel over US-20020042882-A1.

### Obviousness Analysis:

The elements of US-9251332-B2, particularly the wireless personal digital key and reader system with exit-based rules for access termination based on proximity, are not obvious extensions of the

features in US-20020042882-A1. US-20020042882-A1 focuses on access control via passwords and biometrics without the wireless key-reader linkage or proximity-based control, so the claimed invention is not an obvious modification.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20020042882-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a personal digital key adapted for wireless communication within a predefined range to establish a link and send and receive data, | No disclosure of a wireless personal digital key or similar device establishing a wireless link within a predefined range. (Abstract, Description) | Not Found | |
| 2 | the personal digital key associated with a user and storing security data used to access a particular computing resource as described by security set up data for the particular computing resource; | No disclosure of a personal digital key storing security data associated with a user for accessing particular computing resources. (Description) | Not Found | |
| 3 | a reader for automatically detecting the presence of the personal digital key and establishing a link with the personal digital key, | No disclosure of a reader device that automatically detects a personal digital key and establishes a link. (Description) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20020042882-A1 | Status | Explanation |
|---|---|---|---|---|
| 4 | the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | No disclosure of a reader with input/output adapted for wireless communication with a personal digital key within a predefined range. (Description) | Not Found | |
| 5 | the reader automatically signaling a computing device whether it is linked to the personal digital key; | No disclosure of the reader signaling a computing device about linkage status with a personal digital key. (Description) | Not Found | |
| 6 | "the **computing device** having **computing resources** including the particular computing resource," | "US-20020042882-A1 discloses a **computer** with **computing resources**. (Abstract, Description)" | Match | US-20020042882-A1 discloses a computer with computing resources, matching this element. |
| 7 | the computing device coupled to the input and the output of the reader for sending and receiving data; | No disclosure of coupling between computing device and reader for sending/receiving data as claimed. (Description) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20020042882-A1 | Status | Explanation |
|---|---|---|---|---|
| 8 | the computing device including **a security system for controlling access** to the computing resources of the computing device based on security set up data, | US-20020042882-A1 discloses **a security system controlling access** to a computer using passwords and biometrics. (Claims 1, Description) | Partial | US-20020042882-A1 discloses access control but lacks the specific security setup data structure and wireless key-reader system. |
| 9 | wherein the **security set up data is stored in a dedicated encrypted portion of a memory of the computing device** and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | US-20020042882-A1 discloses **embedding encrypted security codes** with data and transferring data in encrypted form. (Claims 1, Description) | Partial | US-20020042882-A1 discloses encrypted data handling but not a dedicated encrypted memory portion storing security setup data separate from security data. |
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | No disclosure of user-defined options for different security actions per resource. (Description) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20020042882-A1 | Status | Explanation |
|---|---|---|---|---|
| 11 | wherein the different security actions include a **biometric confirmation** for a respective computing resource, | US-20020042882-A1 discloses **biometric sensors** for access control. (Claims 1, Description) | Match | US-20020042882-A1 discloses biometric confirmation as a security measure. |
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key, | No disclosure of control based on a signal from a reader linked to a personal digital key. (Description) | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | No disclosure of terminating access based on exit-based rules triggered by loss of proximity between personal digital key and reader. (Description) | Not Found | |

**Rank 14:** US-20070079134-A1 **Priority Date:** 2005-09-23

**Assignee:** Gui-Hua Tang; Wei-Yuan Chen; De-Hua Dang; Zhao-Bin Zhang

**Inventor(s):** Gui-Hua Tang

**Patent Reference:** https://patents.google.com/patent/US20070079134A1

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, including biometric confirmation and exit-based rules for terminating access when the PDK is out of range. US-20070079134-A1 describes a system using a portable storage device connected physically to the computer to store a key for locking/unlocking the computer. US-20070079134-A1 lacks wireless communication, user-defined security actions, biometric confirmation, and exit-based rules based on proximity. The key in US-20070079134-A1 is stored on a portable storage device connected to the computer, not a wireless personal digital key. Thus, US-20070079134-A1 does not capture the core aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20070079134-A1 does not anticipate US-9251332-B2 because it does not disclose or inherently describe a wireless personal digital key communicating within a predefined range, nor does it disclose user-defined security actions or biometric confirmation. The locking/unlocking mechanism in US-20070079134-A1 is based on physical connection of a portable storage device, not wireless proximity detection or exit-based rules. Therefore, US-20070079134-A1 does not disclose all elements of Claim-1 of US-9251332-B2, and thus does not anticipate it under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2 is novel over US-20070079134-A1 because it introduces a wireless personal digital key system with proximity-based access control, user-configurable security actions including biometric confirmation, and exit-based rules for terminating access. US-20070079134-A1 only discloses a portable storage device physically connected to the computer for locking/unlocking, lacking wireless communication, biometric features, and user-defined security actions. Therefore, the novelty of US-9251332-B2 is not invalidated by US-20070079134-A1.

## Obviousness Analysis:

The elements of Claim-1 in US-9251332-B2 are not obvious extensions of US-20070079134-A1. US-20070079134-A1's system is based on a physical portable storage device for key storage and access control, whereas US-9251332-B2 introduces wireless communication, proximity detection, biometric confirmation, and user-defined security actions. These features are not suggested or motivated by US-20070079134-A1, and thus the claimed invention is not obvious over US-20070079134-A1 under 35 U.S.C. §103.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20070079134-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a personal digital key adapted for wireless communication within a predefined range to establish a link and send and receive data, | Portable storage device connected to the computer storing a key (Abstract, Claims) | Not Found | |
| 2 | "the **personal digital key** associated with a user and **storing security data used to access a particular computing resource** as described by security set up data for the particular computing resource;" | "**Key** stored in **portable storage device for computer access** (Claims)" | Partial | US-20070079134-A1 stores a key in a portable device but lacks association with user and detailed security setup data for particular resources. |
| 3 | "a **reader for automatically detecting the presence of the personal digital key** and establishing a link with the personal digital key," | "**Detecting module determines if portable storage device holds key** (Claims)" | Partial | US-20070079134-A1 detects presence of portable storage device but no wireless reader or automatic link establishment. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20070079134-A1 | Status | Explanation |
|---|---|---|---|---|
| 4 | the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | No disclosure of wireless communication or reader input/ output (Description) | Not Found | |
| 5 | the reader automatically signaling a computing device whether it is linked to the personal digital key; | No disclosure of automatic signaling to computing device (Description) | Not Found | |
| 6 | "the **computing device** having **computing resources** including the particular computing resource," | "**Computer** with **computing resources** (Abstract, Description)" | Match | US-20070079134-A1 discloses a computer with computing resources. |
| 7 | "the **computing device** **coupled to the input and the output of the reader** for sending and receiving data;" | "**Portable storage device connected to computer** (Claims)" | Partial | US-20070079134-A1 shows physical connection but no wireless data exchange as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20070079134-A1 | Status | Explanation |
|---|---|---|---|---|
| 8 | the computing device including **a security system for controlling access to the computing resources of the computing device based on security set up data**, | **System locks/unlocks computer based on key presence** (Claims) | Partial | US-20070079134-A1 controls access based on key presence but lacks detailed security setup data and user-defined options. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | No disclosure of dedicated encrypted memory portion or separation of security setup data and security data (Description) | Not Found | |
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | No disclosure of user defined options or different security actions (Description) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20070079134-A1 | Status | Explanation |
|---|---|---|---|---|
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | No disclosure of biometric confirmation (Description) | Not Found | |
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key, | No disclosure of control by signal from reader (Description) | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | No disclosure of exit-based rule or termination based on proximity (Description) | Not Found | |

**Rank 15:** US-20060179057-A1 **Priority Date:** 2005-02-07

**Assignee:** Computerized Security Systems; Inc.

**Inventor(s):** Paolo Moretti

**Patent Reference:** https://patents.google.com/patent/US20060179057A1

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, including biometric confirmation and exit-based rules for terminating access when the PDK is out of range. US-20060179057-A1 describes a security system with a central server and portable client modules that receive access codes for locks, focusing on dynamic access code generation and validation. US-20060179057-A1 lacks the concept of a personal digital key linked directly to a reader and computing device, dedicated encrypted memory storing security setup data excluding security data, and biometric confirmation or exit-based rules based on proximity. The architectures and security mechanisms differ significantly, so US-20060179057-A1 does not capture all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20060179057-A1 does not anticipate US-9251332-B2 because it does not disclose a personal digital key adapted for wireless communication within a predefined range linked to a reader and computing device as described. It lacks the dedicated encrypted memory storing security setup data excluding security data, user-defined security actions including biometric confirmation, and exit-based rules terminating access based on proximity. The server-client model with access codes for locks is fundamentally different from the proximity-based personal digital key system controlling computing resource access in US-9251332-B2.

## Novelty Analysis:

US-9251332-B2 is novel over US-20060179057-A1 because it introduces a unique system architecture involving a personal digital key wirelessly linked to a reader and computing device, with security setup data stored separately from security data, user-configurable security actions including biometrics, and automatic termination of access based on proximity. US-20060179057-A1's focus on server-client access code distribution for locks does not disclose or suggest these features, preserving the novelty of US-9251332-B2.

**Obviousness Analysis:**

The elements of Claim-1 in US-9251332-B2 are not obvious extensions of US-20060179057-A1. US-20060179057-A1's server-client model for access code distribution does not suggest the use of a personal digital key wirelessly linked to a reader and computing device, nor the dedicated encrypted memory with user-defined security actions including biometrics and exit-based rules. The differences in system architecture and security mechanisms indicate that US-9251332-B2's claims are not obvious in light of US-20060179057-A1.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060179057-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | "a **personal digital key adapted for wireless communication within a predefined range** to **establish a link and send and receive data**," | "at least one **client module in wireless communication** with the server module, wherein the client module is portable and **receives an access code from the server module** for unlocking said at least one of said plurality of locks. (Claim 1)" | Partial | Both involve wireless communication with a portable device, but US-20060179057-A1's client module communicates with a server, not a personal digital key linked to a reader and computing device. |
| 2 | "the **personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by **security set up data for the particular computing resource**;" | "a **server module** containing **access information for accessing** a plurality of **locks**; (Claim 1)" | Partial | US-20060179057-A1 stores access information centrally in a server, not in a personal digital key associated with a user. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060179057-A1 | Status | Explanation |
|---|---|---|---|---|
| 3 | a reader for automatically detecting the presence of the personal digital key and establishing a link with the personal digital key, | the portable client module receives an access code from the server module; (Claim 1) | Not Found | |
| 4 | the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | the client module is portable and communicates wirelessly with the server module; (Claim 1) | Not Found | |
| 5 | the reader automatically signaling a computing device whether it is linked to the personal digital key; | the client module communicates with locks and server module; (Claims 1, 9) | Not Found | |
| 6 | the **computing device** having **computing resources** including the **particular computing resource**, | the **plurality of locks** adapted to communicate with the **server module** through the **client module**; (Claim 9) | Partial | US-20060179057-A1 involves locks as resources, but the computing device with computing resources as in US-9251332-B2 is not disclosed. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060179057-A1 | Status | Explanation |
|---|---|---|---|---|
| 7 | the computing device coupled to the input and the output of the reader for sending and receiving data; | the client module forms communication link between server and locks; (Claim 4) | Not Found | |
| 8 | the computing device including **a security system for controlling access** to the computing resources of the computing device based on **security set up data**, | the server module **manages access information** and **validates access codes**; (Claims 1, 10) | Partial | US-20060179057-A1 controls access via server-managed access codes, not via security setup data on the computing device. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | the server module stores access information and generates access codes; (Claims 1, 8) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060179057-A1 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the **security set up data** is based on **one or more user defined options** allowing the user to implement different security actions for different computing resources, | the server module includes **lock configuration** and **user time period applications**; (Claim 5) | Partial | US-20060179057-A1 allows some user-defined options for locks but does not disclose different security actions per computing resource as in US-9251332-B2. |
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | | Not Found | |
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key, | | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | | Not Found | |

**Rank 16:** US-20060107068-A1 **Priority Date:** 2004-11-18

**Assignee:** Michael Fiske

**Inventor(s):** Michael Fiske

**Patent Reference:** https://patents.google.com/patent/US20060107068A1

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, including user-defined security actions like biometric confirmation and exit-based rules for terminating access when the PDK is out of range. US-20060107068-A1 focuses on generating and supplying access keys and passcodes from a secure module to an unsecured system, with no mention of a wireless personal digital key, reader, or proximity-based access control. US-20060107068-A1 lacks the concept of a reader detecting the PDK presence and controlling access based on proximity and user-defined security actions. Therefore, US-20060107068-A1 does not capture all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-20060107068-A1 does not disclose or inherently describe a system comprising a personal digital key adapted for wireless communication within a predefined range, a reader detecting the PDK presence, or a computing device controlling access based on security setup data stored in an encrypted memory with user-defined options including biometric confirmation and exit-based rules. The absence of these key elements means US-20060107068-A1 does not anticipate Claim-1 of US-9251332-B2 under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2 introduces a unique integration of a wireless personal digital key, a reader detecting the key's presence, and a computing device controlling access with user-configurable security actions including biometrics and exit-based rules. US-20060107068-A1, while related to access keys and passcodes, does not disclose this combination or the proximity-based access control system. Thus, US-9251332-B2 remains novel over US-20060107068-A1.

## Obviousness Analysis:

The elements of Claim-1 in US-9251332-B2 involve a wireless personal digital key, a reader detecting presence within a range, and a security system with user-defined options including

biometric confirmation and exit-based rules. US-20060107068-A1 focuses on generating and supplying access keys and passcodes without addressing wireless proximity detection or user-configurable security actions. These differences indicate that the Claim-1 elements are not obvious extensions of US-20060107068-A1's teachings under 35 U.S.C. §103.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060107068-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a personal digital key adapted for wireless communication within a predefined range to establish a link and send and receive data | | Not Found | |
| 2 | the personal digital key associated with a user and storing security data used to access a particular computing resource as described by security set up data for the particular computing resource | | Not Found | |
| 3 | a reader for automatically detecting the presence of the personal digital key and establishing a link with the personal digital key | | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060107068-A1 | Status | Explanation |
|---|---|---|---|---|
| 4 | the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other | | Not Found | |
| 5 | the reader automatically signaling a computing device whether it is linked to the personal digital key | | Not Found | |
| 6 | the **computing device** having **computing resources** including the **particular computing resource** | "the **unsecured system** requires the **access key** to execute a set of instructions or another **entity**" (Abstract) | Partial | US-20060107068-A1 mentions an unsecured system requiring access keys to execute tasks, partially matching the computing device having computing resources. |
| 7 | the computing device coupled to the input and the output of the reader for sending and receiving data | | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060107068-A1 | Status | Explanation |
|---|---|---|---|---|
| 8 | the computing device including a **security system for controlling access to the computing resources of the computing device based on security set up data** | **authenticating the passcode prior to the supplying** (Claim 7) | Partial | US-20060107068-A1 discloses authenticating passcodes before supplying access keys, partially matching controlling access based on security data. |
| 9 | wherein the **security set up data is stored in a dedicated encrypted portion of a memory of the computing device** and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access | "**the secure area does not have an operating system**" (Claim 2) | Partial | US-20060107068-A1 discloses a secure area for storing access keys but does not clearly disclose a dedicated encrypted portion excluding security data used for access. |
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources | | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20060107068-A1 | Status | Explanation |
|---|---|---|---|---|
| 11 | wherein the different security actions include a **biometric confirmation** for a respective computing resource | "generating the access key by applying a one-way function to at least a portion of a **fingerprint**" (Claim 4) | Partial | US-20060107068-A1 mentions generating access keys using biometric data but does not disclose biometric confirmation as a security action for specific computing resources. |
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key | | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range | | Not Found | |

**Rank 17:** US-8359476-B2 **Priority Date:** 1998-05-07

**Assignee:** Empire Ip Llc

**Inventor(s):** Stephen Zizzi

**Patent Reference:** https://patents.google.com/patent/US8359476B2

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to establish a link with a reader, which signals a computing device to control access to computing resources based on security setup data stored in an encrypted memory portion. It includes user-defined security actions such as biometric confirmation and exit-based rules to terminate access when the PDK is out of range. US-8359476-B2 focuses on a biometric user authentication system for encryption/decryption, involving a biometric apparatus, computer-readable medium storing biometric data and encryption keys, and an encryption/decryption computer. It lacks the concept of a personal digital key wirelessly linking to a reader, signaling access control based on proximity, or exit-based rules for terminating access. Thus, US-8359476-B2 does not capture all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-8359476-B2 does not disclose or inherently describe a personal digital key adapted for wireless communication within a predefined range to establish a link with a reader that signals a computing device to control access to computing resources. It also lacks the concept of security setup data stored in a dedicated encrypted portion of memory excluding the security data, user-defined options for different security actions including biometric confirmation, and exit-based rules for terminating access when the key is out of range. Therefore, US-8359476-B2 does not anticipate US-9251332-B2 under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2 introduces a unique integration of a personal digital key wirelessly communicating within a predefined range to a reader, which signals a computing device to control access based on security setup data stored separately from the security data. It includes user-configurable security actions such as biometric confirmation and automatic termination of access based on proximity (exit-based rules). US-8359476-B2, while involving biometric authentication and encryption/decryption, does not disclose these combined features or the wireless proximity-based access control system. Hence, US-9251332-B2 is novel over US-8359476-B2.

### Obviousness Analysis:

The elements of Claim-1 in US-9251332-B2 involve a wireless personal digital key and reader system controlling access based on proximity and user-defined security actions including biometrics and exit-based rules. US-8359476-B2 focuses on biometric authentication for encryption/decryption without any teaching or suggestion of wireless proximity-based access control or exit-based termination rules. There is no obvious extension from US-8359476-B2 to the comprehensive system of US-9251332-B2. Therefore, the claimed invention is not obvious over US-8359476-B2.

### Additional Prior Art from the Same Patent Family:

Apart from US-8359476-B2 whose claim chart is provided below, US-7865728-B2, US-9203626-B2, US-7096358-B2, US-8762713-B2 also belong to the same patent family. These may also aid in the invalidation of the subject patent. These patents disclose similar technical features and concepts that are relevant to the claims of the subject patent, potentially impacting its novelty and inventive step.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-8359476-B2 | Status | Explanation |
|---|---|---|---|---|
| 1 | "a **personal digital key adapted for wireless communication** within a predefined range to establish a link and send and receive data," | "The method of claim 5 further comprising **wirelessly interfacing** with the user authentication apparatus. (Claim 5)" | Partial | US-8359476-B2 discloses wireless interfacing with a biometric authentication apparatus but does not disclose a personal digital key adapted for wireless communication within a predefined range to establish a link and send and receive data as a security token associated with a user. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-8359476-B2 | Status | Explanation |
|---|---|---|---|---|
| 2 | "the **personal digital key associated with a user** and storing **security data used to access a particular computing resource** as described by security set up data for the particular computing resource;" | "A computer-readable medium storing **biometric user identifying information** and **encryption and decryption data**. (Claim 1)" | Partial | US-8359476-B2 stores biometric user identifying information and encryption/ decryption data but does not disclose a personal digital key associated with a user storing security data used to access particular computing resources as described by security setup data. |
| 3 | a reader for automatically detecting the presence of the personal digital key and establishing a link with the personal digital key, | Not Found | Not Found | |
| 4 | the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | Not Found | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-8359476-B2 | Status | Explanation |
|---|---|---|---|---|
| 5 | the reader automatically signaling a computing device whether it is linked to the personal digital key; | Not Found | Not Found | |
| 6 | "the **computing device** having computing resources including the particular computing resource," | "An **encryption and decryption computer** communicating with the user authentication apparatus." | Partial | US-8359476-B2 discloses a computing device (encryption and decryption computer) communicating with the authentication apparatus but does not disclose controlling access to computing resources based on security setup data. |
| 7 | the computing device coupled to the input and the output of the reader for sending and receiving data; | Not Found | Not Found | |
| 8 | the computing device including a security system for controlling access to the computing resources of the computing device based on security set up data, | Not Found | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-8359476-B2 | Status | Explanation |
|---|---|---|---|---|
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | Not Found | Not Found | |
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | Not Found | Not Found | |
| 11 | wherein the different security actions include **a biometric confirmation** for a respective computing resource, | A **biometric user authentication** apparatus; authenticate a user based on the biometric user identifying information. (Claim 1) | Partial | US-8359476-B2 discloses biometric user authentication but does not disclose biometric confirmation as one of multiple user-defined security actions for different computing resources. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-8359476-B2 | Status | Explanation |
|---|---|---|---|---|
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key, | Not Found | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | Not Found | Not Found | |

**Rank 18:** US-7228430-B2 **Priority Date:** 2001-01-11

**Assignee:** Lenovo Singapore Pte. Ltd

**Inventor(s):** Alain Benayoun

**Patent Reference:** https://patents.google.com/patent/US7228430B2

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key that wirelessly communicates within a predefined range to control access to computing resources, including user-defined security actions like biometric confirmation and exit-based rules for terminating access when the key is out of range. US-7228430-B2 focuses on an extractable security piece with a PKI-based mutual authentication system for preventing unauthorized use of a computer, emphasizing cryptographic key exchanges and physical insertion/removal of the security piece. US-7228430-B2 lacks the wireless communication within a predefined range, user-configurable security actions, biometric confirmation, and exit-based access termination based on proximity, which are central to US-9251332-B2's claim. Thus, US-7228430-B2 does not capture all aspects of Claim-1 in US-9251332-B2.

## Anticipation Analysis:

US-7228430-B2 does not anticipate US-9251332-B2 because it does not disclose or inherently describe the wireless communication within a predefined range between a personal digital key and a reader, nor the user-defined security setup data stored in an encrypted portion of memory controlling access with biometric confirmation and exit-based rules. The mutual authentication and PKI infrastructure in US-7228430-B2 are different in nature and do not inherently or expressly disclose the elements of Claim-1 of US-9251332-B2. Therefore, US-7228430-B2 does not anticipate US-9251332-B2 under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2 is novel compared to US-7228430-B2 because it introduces a unique combination of wireless personal digital key communication within a predefined range, a reader signaling linkage status, a security system controlling access based on encrypted user-configurable setup data, and biometric confirmation with exit-based rules for access termination. US-7228430-B2's focus on PKI-based mutual authentication with an extractable security piece does not disclose or suggest these features. Hence, the novelty of US-9251332-B2 is not invalidated by US-7228430-B2.

### Obviousness Analysis:

The elements of Claim-1 in US-9251332-B2 are not obvious extensions of US-7228430-B2. US-7228430-B2's PKI-based extractable security piece and mutual authentication do not suggest wireless communication within a predefined range, user-defined security actions including biometrics, or exit-based rules for terminating access. The technical approaches and security mechanisms differ significantly, and there is no motivation or teaching in US-7228430-B2 that would render US-9251332-B2's claims obvious under 35 U.S.C. §103.

### Additional Prior Art from the Same Patent Family:

Apart from US-7228430-B2 whose claim chart is provided below, EP-1379930-B1 also belong to the same patent family. These may also aid in the invalidation of the subject patent. These patents disclose similar technical features and concepts that are relevant to the claims of the subject patent, potentially impacting its novelty and inventive step.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-7228430-B2 | Status | Explanation |
|---|---|---|---|---|
| 1 | a personal digital key adapted for wireless communication within a predefined range to establish a link and send and receive data, | An extractable security piece which can be removed from the main computer device by the authorized user, wherein the extractable security piece includes an extractable main private key and a main PC public key; (Claim 1) | Not Found | |
| 2 | "the **personal digital key associated with a user** and **storing security data used to access a particular computing resource** as described by **security set up data for the particular computing resource**;" | "The **extractable security piece** includes a **password that is used by said computer device and that is exchanged** with a **password included in said PC security area**. (Claim 2)" | Partial | US-7228430-B2 stores security data (password) in the extractable piece but lacks description of user association and security setup data for particular computing resources. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-7228430-B2 | Status | Explanation |
|---|---|---|---|---|
| 3 | a **reader for automatically detecting the presence of the personal digital key** and establishing a link with the personal digital key, | **Processing means in said extractable security piece and in said PC security area for mutual authentication** of said extractable security piece and said PC security area (Claim 1) | Partial | US-7228430-B2 discloses mutual authentication but not automatic detection or wireless link establishment as in US-9251332-B2. |
| 4 | the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | No explicit disclosure of wireless communication or reader input/ output adapted for wireless communication. (Description) | Not Found | |
| 5 | the reader automatically signaling a computing device whether it is linked to the personal digital key; | No explicit disclosure of signaling the computing device about linkage status. (Description) | Not Found | |
| 6 | the **computing device** having computing resources including the particular computing resource, | **Main computer device** having an authorized user (Abstract) | Partial | US-7228430-B2 discloses a main computer device but does not detail computing resources as in US-9251332-B2. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-7228430-B2 | Status | Explanation |
|---|---|---|---|---|
| 7 | the computing device coupled to the input and the output of the reader for sending and receiving data; | No explicit disclosure of coupling computing device to reader input/ output for data exchange. (Description) | Not Found | |
| 8 | the computing device including **a security system** for **controlling access to the computing resources of the computing device** based on security set up data, | **Security system** for **preventing unauthorized use of a computer device** (Title, Abstract) | Partial | US-7228430-B2 discloses a security system but based on PKI and mutual authentication, not on security setup data as in US-9251332-B2. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | No explicit disclosure of dedicated encrypted memory portion storing security setup data excluding security data. (Description) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-7228430-B2 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | No disclosure of user defined options or different security actions for different computing resources. (Description) | Not Found | |
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | No disclosure of biometric confirmation. (Description) | Not Found | |
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key, | No disclosure of control by signal from reader indicating linkage. (Description) | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | No disclosure of exit-based rule terminating access when key and reader are out of range. (Description) | Not Found | |

**Rank 19:** EP-1564625-A1 **Priority Date:** 2004-02-17

**Assignee:** Hewlett-Packard Development Company; L.P.

**Inventor(s):** Matthew J. Wagner

**Patent Reference:** https://patents.google.com/patent/EP1564625A1

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, including user-defined security actions like biometric confirmation and exit-based rules for terminating access when the PDK is out of range. EP-1564625-A1 focuses on a self-managed device with an authentication system and a security module that authenticates a user and generates device credential data transparently to the user. EP-1564625-A1 lacks any mention of a wireless personal digital key, proximity-based access control, or user-defined security actions including biometrics. The concepts and mechanisms in EP-1564625-A1 do not capture the key aspects of US-9251332-B2's claim 1.

## Anticipation Analysis:

EP-1564625-A1 does not disclose or inherently describe a personal digital key adapted for wireless communication within a predefined range, nor a reader that detects the presence of such a key and signals a computing device accordingly. It also lacks disclosure of security setup data stored in a dedicated encrypted memory portion with user-defined options and exit-based rules. Therefore, EP-1564625-A1 does not anticipate the elements of claim 1 of US-9251332-B2 under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2's novelty lies in the integration of a wireless personal digital key, a reader that detects the key's presence and signals the computing device, and a security system that uses encrypted setup data with user-configurable security actions including biometrics and exit-based rules. EP-1564625-A1 does not disclose these features or their combination, thus US-9251332-B2 remains novel over EP-1564625-A1.

## Obviousness Analysis:

The elements of claim 1 in US-9251332-B2 involve a unique combination of wireless proximity detection, user-configurable security actions including biometrics, and exit-based access

termination, which are not suggested or rendered obvious by the teachings of EP-1564625-A1. EP-1564625-A1's focus on transparent generation of device credential data without wireless key detection or proximity-based control does not make US-9251332-B2's claims obvious under 35 U.S.C. §103.

### Additional Prior Art from the Same Patent Family:

Apart from EP-1564625-A1 whose claim chart is provided below, US-7581111-B2 also belong to the same patent family. These may also aid in the invalidation of the subject patent. These patents disclose similar technical features and concepts that are relevant to the claims of the subject patent, potentially impacting its novelty and inventive step.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in EP-1564625-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a personal digital key adapted for wireless communication within a predefined range to establish a link and send and receive data, | No mention of a personal digital key or wireless communication within a predefined range. EP-1564625-A1 focuses on a security module and authentication system without wireless key. | Not Found | |
| 2 | the personal digital key associated with a user and storing security data used to access a particular computing resource as described by security set up data for the particular computing resource; | No disclosure of a personal digital key storing security data associated with a user for accessing computing resources. | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in EP-1564625-A1 | Status | Explanation |
|---|---|---|---|---|
| 3 | a reader for automatically detecting the presence of the personal digital key and establishing a link with the personal digital key, | No mention of a reader device that detects a personal digital key or establishes a link with it. | Not Found | |
| 4 | the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | No disclosure of a reader with input/output adapted for wireless communication with a personal digital key within a predefined range. | Not Found | |
| 5 | the reader automatically signaling a computing device whether it is linked to the personal digital key; | No disclosure of the reader signaling a computing device about linkage to a personal digital key. | Not Found | |
| 6 | the **computing device** having **computing resources** including the particular computing resource, | EP-1564625-A1 discloses a self-managed **device** with **computing resources** controlled by an authentication system. | Partial | EP-1564625-A1 discloses a computing device with resources but lacks the specific context of the personal digital key and reader. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in EP-1564625-A1 | Status | Explanation |
|---|---|---|---|---|
| 7 | the computing device coupled to the input and the output of the reader for sending and receiving data; | No disclosure of coupling between a computing device and a reader for sending/receiving data. | Not Found | |
| 8 | the computing device including **a security system for controlling access to the computing resources of the computing device** based on **security set up data**, | EP-1564625-A1 discloses **an authentication system controlling access to the device**, but no mention of **security set up data** as in US-9251332-B2. | Partial | EP-1564625-A1 has an authentication system but lacks the specific security set up data concept. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | No disclosure of security set up data stored in a dedicated encrypted memory portion excluding security data used for access. | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in EP-1564625-A1 | Status | Explanation |
|---|---|---|---|---|
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | No disclosure of user defined options for different security actions for different computing resources. | Not Found | |
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | No mention of biometric confirmation as a security action. | Not Found | |
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key, | No disclosure of security system controlled by a reader signal indicating linkage to a personal digital key. | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | No disclosure of terminating access based on exit-based rules triggered by loss of proximity between personal digital key and reader. | Not Found | |

**Rank 20:** US-20050182944-A1 **Priority Date:** 2004-02-17

**Assignee:** Wagner Matthew J.; Valiuddin Ali; Manuel Novoa

**Inventor(s):** Matthew Wagner

**Patent Reference:** https://patents.google.com/patent/US20050182944A1

## Similarity Analysis:

US-9251332-B2 describes a system with a personal digital key (PDK) that wirelessly communicates within a predefined range to control access to computing resources, including user-defined security actions like biometric confirmation and exit-based rules for terminating access when the PDK is out of range. US-20050182944-A1 focuses on a self-managed device with an authentication system that automatically generates device credential data transparently to the user for access control. US-20050182944-A1 lacks any mention of a personal digital key, wireless communication within a predefined range, reader devices, or user-defined security actions including biometrics or exit-based rules. The concepts and system architectures differ significantly, indicating no capture of all aspects of Claim-1 in US-9251332-B2 by US-20050182944-A1.

## Anticipation Analysis:

US-20050182944-A1 does not disclose or inherently describe the key elements of Claim-1 of US-9251332-B2, such as a personal digital key adapted for wireless communication within a predefined range, a reader detecting the key's presence, or security setup data stored in a dedicated encrypted portion excluding the security data itself. The automatic generation of device credential data in US-20050182944-A1 is distinct from the wireless key-reader system and user-configurable security actions in US-9251332-B2. Therefore, US-20050182944-A1 does not anticipate US-9251332-B2 under 35 U.S.C. §102.

## Novelty Analysis:

US-9251332-B2 introduces a unique integration of a personal digital key wirelessly communicating within a predefined range, a reader device signaling the computing device, and a security system with user-defined options including biometric confirmation and exit-based rules. US-20050182944-A1's focus on automatic generation of device credential data for a self-managed device does not disclose or suggest these features. Thus, US-9251332-B2 retains novelty over US-20050182944-A1 as these novel elements are not found or suggested in US-20050182944-A1.

**Obviousness Analysis:**

The elements of Claim-1 in US-9251332-B2 involve a wireless personal digital key and reader system with user-configurable security actions and exit-based rules, which are not suggested or rendered obvious by the automatic credential generation and authentication system of US-20050182944-A1. The technical approaches and system components differ substantially, and there is no motivation or teaching in US-20050182944-A1 that would lead one skilled in the art to combine or modify its teachings to arrive at the system of US-9251332-B2. Therefore, the claim elements are not obvious extensions of US-20050182944-A1.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20050182944-A1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a personal digital key adapted for wireless communication within a predefined range to establish a link and send and receive data, | No disclosure of a personal digital key or wireless communication within a predefined range; US-20050182944-A1 focuses on device credential generation and authentication within a self-managed device. (Abstract, Claims) | Not Found | |
| 2 | the personal digital key associated with a user and storing security data used to access a particular computing resource as described by security set up data for the particular computing resource; | US-20050182944-A1 describes device credential data generated for user authentication but does not describe a personal digital key storing security data for particular computing resources. (Claims) | Not Found | |
| 3 | a reader for automatically detecting the presence of the personal digital key and establishing a link with the personal digital key, | No mention of a reader device detecting a personal digital key; US-20050182944-A1 focuses on authentication within a self-managed device. (Claims, Abstract) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20050182944-A1 | Status | Explanation |
|---|---|---|---|---|
| 4 | the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, | No disclosure of reader input/ output or wireless communication with a personal digital key. (Claims) | Not Found | |
| 5 | the reader automatically signaling a computing device whether it is linked to the personal digital key; | No disclosure of signaling from a reader to a computing device about linkage to a personal digital key. (Claims) | Not Found | |
| 6 | the **computing device** having **computing resources** including the particular **computing resource**, | US-20050182944-A1 describes a self-managed **device** with **computing resources** controlled by an authentication system. (Abstract, Claims) | Partial | US-20050182944-A1 discloses a self-managed device with computing resources but lacks the specific context of the personal digital key system. |
| 7 | the computing device coupled to the input and the output of the reader for sending and receiving data; | No disclosure of coupling between a computing device and a reader for data communication. (Claims) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20050182944-A1 | Status | Explanation |
|---|---|---|---|---|
| 8 | the computing device including **a security system for controlling access** to the computing resources of the computing device based on security set up data, | US-20050182944-A1 discloses **an authentication system controlling access** to a self-managed device. (Claims) | Partial | US-20050182944-A1 discloses access control but not based on security setup data as defined in US-9251332-B2. |
| 9 | wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, | No disclosure of security setup data stored separately excluding security data used for access. (Claims, Description) | Not Found | |
| 10 | wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, | No disclosure of user-defined options for different security actions per computing resource. (Claims) | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in US-20050182944-A1 | Status | Explanation |
|---|---|---|---|---|
| 11 | wherein the different security actions include a biometric confirmation for a respective computing resource, | No disclosure of biometric confirmation as a security action. (Claims) | Not Found | |
| 12 | the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key, | No disclosure of control based on signals from a reader linked to a personal digital key. (Claims) | Not Found | |
| 13 | and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | No disclosure of exit-based rules terminating access when a personal digital key is out of range. (Claims, Description) | Not Found | |

# Non-Patent Literature

This section presents a collection of academic publications and scientific articles that relate to the subject patent. These references provide additional insights that may contribute to a broader understanding or assessment of the invention.

**Rank 1:** 0712.2231v1 **Published:** 2007-12-13

**Cited Research:** https://arxiv.org/pdf/0712.2231v1

### NPL Source:

This document references a preprint archived on arXiv, originally associated with the following information: **To appear in: Proceedings of the Wireless Communications and Networking Conference, IEEE WCNC 2008, Las Vegas, USA, 31 March - 2 April 2008**. Please note that arXiv content may not have been peer-reviewed at the time of access.

### Similarity Analysis:

The 0712.2231v1 describes a system for location-based authorization using a mobile device with trusted computing capabilities, including a location trigger enforcer (LTE) that enforces policies based on the device's location. The 0712.2231v1's system involves a mobile device (MT) that communicates with network elements (eNBs, AGW) and a trusted location trigger authorization center (TLTAC). The device detects its presence within a protected zone and enforces policies accordingly. This conceptually overlaps with the US-9251332-B2's system comprising a personal digital key (PDK), a reader, and a computing device controlling access based on proximity and security setup data. Both systems involve wireless communication within a predefined range, detection of presence, and enforcement of access control policies based on that presence. However, the 0712.2231v1 focuses on location-based authorization using GPS and network cell information, while US-9251332-B2 focuses on a personal digital key and reader system with encrypted security setup data and biometric confirmation. The 0712.2231v1 does not explicitly disclose a personal digital key storing security data, a reader signaling the computing device, or the specific encrypted security setup data with user-defined options including biometric confirmation. Therefore, the similarity is partial and conceptual but not a direct match in all technical details.

### Anticipation Analysis:

The 0712.2231v1 does not explicitly or inherently disclose all elements of Claim-1 of US-9251332-B2. Specifically, the 0712.2231v1 lacks disclosure of a personal digital key adapted for wireless communication storing security data used to access particular computing resources as described by security setup data. It also does not disclose a reader device that automatically detects the presence of the personal digital key and signals the computing device. The 0712.2231v1's system is based on location-based authorization using trusted computing and GPS, which is different from the personal digital key and reader system controlling access based on

proximity and encrypted security setup data. Therefore, the 0712.2231v1 does not anticipate the claimed invention as it does not disclose all claim elements either expressly or inherently.

### Novelty Analysis:

US-9251332-B2 is novel over the 0712.2231v1 because the 0712.2231v1 does not disclose the unique combination of a personal digital key storing security data, a reader that detects the key and signals the computing device, and a security system using encrypted security setup data with user-defined options including biometric confirmation. The 0712.2231v1's focus on location-based authorization using GPS and trusted computing does not teach or suggest these specific features. Thus, the claimed invention presents novel features not found in the 0712.2231v1.

### Obviousness Analysis:

While the 0712.2231v1 discloses location-based authorization and trusted computing concepts, it does not explicitly disclose or suggest the use of a personal digital key and reader system with encrypted security setup data and biometric confirmation as claimed. However, one could argue that combining location-based authorization with personal digital key systems might be an obvious extension to a person skilled in the art. The lack of explicit disclosure of the claimed features in the 0712.2231v1 makes obviousness uncertain without further evidence or combination with other prior art.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in 0712.2231v1 | Status | Explanation |
|---|---|---|---|---|
| 1 | a **personal digital key adapted for wireless communication** within a predefined range to establish a link and send and receive data, the **personal digital key associated with a user and storing security data used to access a particular computing resource** as described by security set up data for the particular computing resource | The 0712.2231v1 describes a **mobile device (MT) with trusted computing capabilities that communicates wirelessly** and enforces policies based on location, but does not disclose a separate **personal digital key storing security data for accessing computing resources**. [Abstract, Section II] | Partial | Conceptually similar in wireless communication and user association, but no explicit personal digital key storing security data is disclosed. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in 0712.2231v1 | Status | Explanation |
|---|---|---|---|---|
| 2 | a reader for automatically detecting the presence of the personal digital key and establishing a link with the personal digital key, the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, the reader automatically signaling a computing device whether it is linked to the personal digital key | The 0712.2231v1 describes network elements (eNBs, AGW) that interact with the mobile device and enforce policies, but does not disclose a reader device that detects a personal digital key and signals a computing device. [Section II, Figures 1-6] | Not Found | |

| | | | | |
|---|---|---|---|---|
| 3 | the computing device having computing resources including the particular computing resource, the computing device coupled to the input and the output of the reader for sending and receiving data; the computing device including **a security system** for controlling access to the computing resources of the computing device based on **security set up data**, wherein the **security set up data** is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, wherein the **security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources**, wherein | The 0712.2231v1 describes **a security system** enforcing location-based policies on a mobile device, with policy enforcement based on location triggers and trusted computing, but does not disclose encrypted **security setup data** excluding security data, **user-defined options for different security actions**, **biometric confirmation**, or **exit-based rules based on proximity of a personal digital key and reader**. [Sections II, III] | Partial | Similar concept of policy enforcement and access control, but missing specific features of encrypted security setup data, biometric confirmation, and exit-based rules tied to a personal digital key and reader. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in 0712.2231v1 | Status | Explanation |
|---|---|---|---|---|
| | the different security actions include **a biometric confirmation for a respective computing resource**, the **security system** controlled by the signal from the reader indicating whether the reader is linked to the personal digital key and terminating access to the computing resource based on **an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range**. | | | |

**Rank 2:** 0707.2293v1 **Published:** 2007-07-16

**Cited Research:** https://arxiv.org/pdf/0707.2293v1

### NPL Source:

This document references a preprint archived on arXiv, originally associated with the following information: **Published in New J. Phys. 9 189, 2007**. Please note that arXiv content may not have been peer-reviewed at the time of access.

### Similarity Analysis:

The 0707.2293v1 primarily discusses the propagation of computer worms in wireless adhoc networks, focusing on the modeling of worm spread dynamics, network topology, and medium access control mechanisms. It describes how devices communicate wirelessly within a range and how worms spread via multihop broadcasts. However, it does not disclose or describe a security system comprising a personal digital key (PDK) adapted for wireless communication within a predefined range to establish a link and send/receive data, a reader that automatically detects the PDK and signals a computing device, or a computing device with a security system controlling access based on security setup data stored in a dedicated encrypted memory portion. The 0707.2293v1 lacks any mention of a security system that controls access to computing resources based on proximity of a personal digital key, biometric confirmation, or exit-based rules for terminating access. Therefore, the 0707.2293v1 does not capture the technical ideas or system architecture claimed in Claim-1 of US-9251332-B2.

### Anticipation Analysis:

Anticipation requires that all elements of the claimed invention be disclosed, either explicitly or inherently, in a single prior art reference. The 0707.2293v1 does not disclose a personal digital key storing security data, a reader detecting the key and signaling a computing device, or a security system controlling access to computing resources based on security setup data with user-defined options including biometric confirmation and exit-based rules. The 0707.2293v1 focuses on worm propagation models and wireless network communication characteristics, not on access control systems or security architectures. Hence, the 0707.2293v1 does not anticipate the claimed invention in US-9251332-B2.

### Novelty Analysis:

US-9251332-B2 introduces a novel security system integrating a personal digital key for wireless communication, a reader that detects the key and signals a computing device, and a security system controlling access to computing resources based on encrypted security setup data with

user-configurable security actions including biometric confirmation and exit-based rules. The 0707.2293v1 does not disclose or suggest such a system or method. Therefore, the claimed invention in US-9251332-B2 is novel over the 0707.2293v1.

### Obviousness Analysis:

The 0707.2293v1 discusses wireless communication and worm propagation in adhoc networks but does not address security systems controlling access to computing resources using a personal digital key and reader setup as claimed. There is no teaching or suggestion in the 0707.2293v1 that would motivate a person skilled in the art to combine the worm propagation models with a security system comprising a personal digital key, reader, and computing device with encrypted security setup data and biometric confirmation. The technical fields and purposes differ significantly. Thus, the claimed invention is not an obvious extension of the ideas in the 0707.2293v1.

## Claim Chart

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in 0707.2293v1 | Status | Explanation |
|---|---|---|---|---|
| 1 | "a **personal digital key adapted for wireless communication within a predefined range** to establish a link and send and receive data, the **personal digital key associated with a user and storing security data used to access a particular computing resource** as described by security set up data for the particular computing resource;" | "The 0707.2293v1 discusses **wireless communication between devices within a certain range** (e.g., WiFi or Bluetooth) and the propagation of worms via multihop broadcasts in wireless adhoc networks [Abstract, Section II.A]. However, it does not disclose a **personal digital key associated with a user that stores security data for accessing computing resources**." | Partial | Similar concept of wireless communication within a range exists, but no disclosure of a personal digital key storing security data for access control. |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in 0707.2293v1 | Status | Explanation |
|---|---|---|---|---|
| 2 | a reader for automatically detecting the presence of the personal digital key and establishing a link with the personal digital key, the reader having an input and an output and adapted for wireless communication with the personal digital key when the reader and the personal digital key are within the predefined range of each other, the reader automatically signaling a computing device whether it is linked to the personal digital key; | The 0707.2293v1 describes devices communicating wirelessly and the concept of transmission range and links between devices [Section II.A]. However, it does not disclose a reader device that detects a personal digital key and signals a computing device about the link status. | Not Found | |

| | | | | |
|---|---|---|---|---|
| 3 | the computing device having computing resources including the particular computing resource, the computing device coupled to the input and the output of the reader for sending and receiving data; the computing device including a security system for controlling access to the computing resources of the computing device based on security set up data, wherein the security set up data is stored in a dedicated encrypted portion of a memory of the computing device and includes information on how to control access to the computing resources using security data, but does not include the security data used to obtain access, wherein the security set up data is based on one or more user defined options allowing the user to implement different security actions for different computing resources, wherein | The 0707.2293v1 focuses on worm propagation and network communication models and does not disclose any computing device with a security system controlling access to computing resources based on encrypted security setup data, user-defined security actions, biometric confirmation, or exit-based rules for terminating access [Entire 0707.2293v1]. | Not Found | |

| # | Element of Claim 1 in US-9251332-B2 | Corresponding content in 0707.2293v1 | Status | Explanation |
|---|---|---|---|---|
| | the different security actions include a biometric confirmation for a respective computing resource, the security system controlled by the signal from the reader indicating whether the reader is linked to the personal digital key and terminating access to the computing resource based on an exit-based rule of the security set up data associated with the computing resource when the personal digital key and the reader are no longer within the predefined range. | | | |