

DIRECTIONAL SENSING MECHANISM AND COMMUNICATIONS AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Patent Application Ser. No. 61/087,633, filed Aug. 8, 2008, the entire disclosure of which is hereby incorporated herein by reference.

FIELD OF THE INVENTION

[0002] The present invention is generally directed to the detection of card movement and the utilization of said detection information in connection with controlling operation thereof.

BACKGROUND

[0003] Radio Frequency Identification (RFID) systems use an RFID reader to wirelessly detect the presence of a nearby RFID tag and read an identification code stored in the tag. The identification code in the RFID tag can be used to control access to a protected resource by allowing access only when an RFID tag having an authorized identification code is detected. Generally, the authorized RFID tag is issued to an authorized user to ensure that only the authorized user has access to the protected resource. If the authorized RFID tag is lost or stolen, however, it can be presented by an unauthorized user to access the protected resource.

[0004] Presently available installed RFID systems use a variety of different complex coding and signaling methods, some of which are proprietary. The RFID tags used with these systems take two forms—cards and key fobs. The coding that these leased programmers can embed is limited to certain specific ranges and formats allowed by each of the distributors and controlled by an encrypted media, which is supplied by each of the companies.

[0005] There are proposals to integrate RFID devices into banknotes, credit cards, debit cards, store loyalty cards and other high-value objects in an attempt to prevent fraud. The thought is that a person carrying an object with all of the authentication information must be the true object owner. As more and more objects are equipped with these RFID devices, the chances of having one's personal information stolen from them increases. High-value objects integrated with RFID devices typically carry extremely sensitive information (e.g. social security numbers, addresses, bank account numbers, ATM pin codes, names, etc.) If this type of information is stolen, the entire identity of the object holder may be compromised. This poses a very serious threat to the general population carrying objects equipped with an RFID device.

SUMMARY

[0006] It is, therefore, one aspect of the present invention to provide an RFID device that restricts data transmissions until it has been moved in a particular way by the holder of the RFID device. By requiring the holder of the device to move the RFID device in a certain way before releasing its sensitive data, the RFID device potentially limits its use, and therefore release of sensitive data, to instances where an authorized user is actually presenting the card purposefully to a reader (assuming that an unauthorized user does not know the predetermined motion sequence that unlocks the sensitive data from the RFID device). This helps minimize or completely

prevent third parties from stealing data from the RFID device unless the holder of the RFID device is moving it in the predetermined sequence of motions. In other words, an attacker is restricted from illicitly passing a reader in proximity to the user's RFID device to harvest data from the user without their consent.

[0007] In accordance with at least one embodiment of the present invention, an RFID device is equipped with a directional sensing mechanism such as a Micro-Electro-Mechanical System (MEMS) or accelerometer that is capable of sensing movement of the RFID device in one or more directions and/or rotations of the RFID device in one or more rotational directions. The present invention is generally directed toward a method, apparatus, and system that utilizes a directional sensing component in combination with an RFID device to substantially prohibit illicit data harvesting from RFID devices. As can be appreciated, an RFID device can be implemented as a part of an ID/access card, smart card, RF tag, cellular phone, Personal Digital Assistant (PDA), key fob, and the like.

[0008] In accordance with one embodiment of the present invention, a system is provided that substantially prevents the illegitimate harvesting of data from an RFID device. The data may have degrees of sensitivity. For example, highly sensitive data may include, but is not limited to, bank account numbers, social security numbers, PIN codes, passwords, keys, RFID unique ID, encryption schemes, etc. Less sensitive data may include, but is not limited to, user name, manufacturer ID, job title, and so on.

[0009] MEMS are the integration of mechanical elements, sensors, actuators, and electronics on a common silicon substrate through microfabrication technology. While the electronics are fabricated using integrated circuit (IC) process sequences (e.g., CMOS, Bipolar, or BICMOS processes), the micromechanical components are fabricated using compatible "micromachining" processes that selectively etch away parts of the silicon wafer or add new structural layers to form the mechanical and electromechanical devices.

[0010] MEMS are capable of bringing together silicon-based microelectronics with micromachining technology, making possible the realization of complete systems-on-a-chip. MEMS is an enabling technology allowing the development of smart products, augmenting the computational ability of microelectronics with the perception and control capabilities of microsensors and microactuators and expanding the space of possible designs and applications.

[0011] Because MEMS devices are manufactured using batch fabrication techniques similar to those used for integrated circuits, unprecedented levels of functionality, reliability, and sophistication can be placed on a small silicon chip at a relatively low cost.

[0012] In accordance with at least some embodiments of the present invention, the MEMS device may be provided as an integral part of the processing chip that is also used to control the RF communication functionality of the RFID device. More specifically, a single chip may be responsible for executing the traditional processing of the RFID device as well as controlling whether the RFID device is allowed to respond to a request for data from a reader (or even enable the antenna to respond to any type of RF field). Unless the proper sequence of motions (e.g., rotations, sliding motions, etc.) is detected by the MEMS device the processor will not be allowed to reveal any sensitive data from its storage location on the RFID device. In accordance with at least one embodi-