TECHNICAL INSIGHTS

SENSOR

TECHNOLOGY ALERT

12th September 2014

1. BIOMETRIC ACCESS CARDS FOR ENHANCED SECURITY

The three methods generally employed for access control are personal identification number (PIN), access cards, and biometrics. These three systems are subjected to certain challenges that limit their versatility in different applications. PIN-based and access card-based solutions do not confirm the individual's credentials; they only ascertain if the card is authorized or the PIN number is correct. Access cards and PIN numbers can be stolen and used by other individuals to gain access to restricted areas. Biometric-based systems, on the other hand, are less susceptible to these security breaches as they confirm the user's unique attributes. However, biometric-based systems are expensive when it comes to implementation. Thus, there is a need for a solution that provides enhanced security and is cost-effective at the same time.

Norway-based Zwipe has come up with an innovative solution that integrates the secure aspect of biometrics with the flexibility of implementation of an access card solution. The company's solution provides a fingerprint sensing and authentication system inside a normal access card. The Zwipe card has been designed similar to a normal access card. In addition, it contains a capacitive fingerprint sensor on which the user needs to place his finger to authenticate his credentials. The Zwipe card is similar in size to conventional access cards and can be personalized with employee details and photograph.

Fingerprint sensing is the most mature technology in biometrics; and Zwipe has used the proven capacitive fingerprint-sensing technology of Fingerprint Cards AB (FPC), Sweden. The card uses MIFARE Classic and MIFARE DESFire EV1 chips from NXP Semiconductors, which are known for their low cost and reliability. Zwipe has leveraged FPC's three-dimensional (3D) capacitive fingerprint-sensing solution inside an access card where the authentication happens on the card itself. If a match occurs, the card transmits the tag ID to the reader. The card is ISO 14443 compatible, making it usable

with already available card readers. This makes the Zwipe system easy and cost-effective for implementation.

The Zwipe access control card can be used to provide an easy upgrade to existing security solutions. In large organizations, the card can be issued to employees who need to access highly secure areas. Biometric information is stored in the card, which makes it a secure system. Since only the owner of the card can operate it, threats of stolen cards are negated. The authentication happens in less than one second, which is extremely fast. The most important benefit of the Zwipe card is that users need not remember complex passwords and PIN numbers and can employ a highly secure access control system.

The next generation of Zwipe's offerings will include cards that are less costly and thinner than the current cards. Zwipe has already received private funding as well as support from the Norwegian Government for product development and commercialization.

Details: Kim Kristian Humborstad, CEO, Zwipe AS, Tollbugata 13, postkasse 361, 0152 Oslo, Norway. Phone: +47-922-52-006. E-mail:kim@zwipe.com. URL: www.zwipe.no

2. SENSORS ENABLING SMART ENVIRONMENTS

Technology is evolving at a fast pace and changing people's day to day life. Information and communication technologies (ICT) can be used with any device that is Internet enabled. We are entering the era of the Internet-of-Things (IoT). Devices are becoming more powerful, smaller and permanently networked to provide multitude of real-time information about the condition of the device or the environment. Technology is entering our home and life and making the environment smart. These technologies are developed with very complex mechanisms and networks. There is a need for a process or a device to be utilized for the Internet–of-Things that can be operated with ease. It should be efficient and capable of multitasking.

Germany-based company Relayr has developed the WunderBar, a starter kit for the Internet-of-Things. It is a set of wireless detachable sensors, which can be monitored and controlled through the smart phone and communicated through the Internet. The WunderBar comprises a microprocessor, USB, Bluetooth, and set of sensors.

The researchers from Relayr have developed WunderBar by deploying different sensors, such as accelerometers and proximity, humidity and Infrared (IR) transmitters. The sensors can be easily detached from the bar and used for the appropriate purpose. The accelerometer can be detached from the bar and placed on a cycle to track the progress of the user. With the appropriate application designed with the help of the microprocessor, it can update the user about the total calories burnt after an exercise session. The main module comprises a microprocessor. The microprocessor is used to interpret the data collected by the sensors and provide an update to the smartphones through the Wi-Fi unit. The sensor modules communicate with each other through Bluetooth.

In the initial stages, the product will be used for making home and office environments smart and intelligent. It will allow users to control electronic appliances with the help of the IR transmitter, for instance, the user can easily switch the air conditioner on or off. The device will also be used to share networks with the other devices through its crowd sourced sensors. In the future, WunderBar will be utilized for many different applications for the Internet-of-Things.

This project was crowd funded with the help of dragon innovation. The Relayr team is working on building up the level of security in its device. In the future, the team is also planning to implement 3D printing for the manufacture of the device. Relayr is looking to generate funds by partnering with organizations. The product is available in the marketplace, and has opportunities to be well received by end users as it is easy to use and efficient.

Details: Harald Zapp, CEO, Relayr, Rainmaking Loft, Charlottenstrasse 2, 10969 Berlin, Germany; Phone: +49-0-179-2989-866. E-mail: info@relayr.io, URL:https://relayr.io/team

3. PAPER-THIN VIBRATION ACTUATORS FOR HAPTICS AND SENSING

Conventional haptic feedback systems have relied on vibration feedback using eccentric rotating mass actuators, which have a relatively high mechanical time constant, and bulky linear resonator actuators (LRAs). The major challenges faced by these vibrators include bulkiness in size, and inability to provide localized vibrations. With the trend of miniaturization in electronics, smartphones, tablets and keyboards are becoming thinner with every version.

There is thus a need for components that are able to fit inside low space constraints of next-generation consumer electronics devices.

Novasentis, USA, has developed an innovative haptics technology that can also be used as a pressure sensor using ferroelectric electro-mechanical polymer (EMP) technology. The technology enables paper-thin vibration actuators with superior tensile and elastic properties with the potential to transform the user's experience by means of localized haptic feedback in a wide spectrum of products.

Novasentis' EMP is essentially a piezoelectric polymer that elongates when an electric field is applied across it. It can also generate an electric charge when deformed by a physical force. When this polymer is attached to a substrate and an electric field is applied to the polymer, the polymer expands and as a result, the actuator also bends. This motion can create vibrations within a large frequency spectrum that ranges from about 0 Hz to 500 Hz and also emits sound simultaneously. The EMP actuators can have thickness of less than 120 micrometers, which enables the devices to fit into a variety of tight spaces. This opens up opportunities for innovative applications using haptic capability as a key component.

The EMP technology has the potential to benefit various product segments in areas such as consumer electronics, automotive infotainment, healthcare, and medical devices. The technology enables ultra-thin keyboards to have localized feedback that users are currently unable to experience in conventional touchscreen interfaces. The smartphone market is another area where Novasentis' technology can have vast opportunities. It can enable a whole new paradigm of experience in gaming, typing, and user interactions. The EMP technology can also be used to develop thinner and less expensive Braille displays for people with visual impairments. In the automotive area, haptic feedback can be used in controlling in-car infotainment and navigation. When the actuators are operated at levels below 100 Hz, they can be integrated into audio systems, such as sub-woofers and headphones. In addition, the technology can be used as sensors. Because the polymer is piezoelectric in nature, it can convert input pressure or touch into a voltage.

Novasentis' first product, the Clic 1010 actuator, should be incorporated into commercial products around 2015, and Novasentis plans to scale up its manufacturing capabilities to meet the high volume of demand expected for the

product. Currently, the technology is used to manufacture actuators that are opaque. However, transparent versions of the actuator are expected to be commercialized by 2016.

Details: Christophe Ramstein, President and CEO, Novasentis Inc., 1350 Old Bayshore Hwy, Suite 450, Burlingame, CA 94010. Phone: +1-410-802-6999. E-mail: cramstein@novasentis.com. URL: www.novasentis.com.

4. RECENT PATENTS IN THE FIELD OF FINGERPRINT SENSORS

One of the methods for personal identification is biometric authentication. Biometric authentication systems are used to identify unique human behavioral and physiological characteristics, such as iris, vein, face, fingerprint and palm. The process of biometric authentication involves comparing the biometrics of the present user with an already existing database of biometrics. Comparison will allow the system to, for example, match user fingerprints with the existing prints in the database. Thus, the system can determine whether the user is legitimate or not. To collect digital images of finger prints, the key fingerprint sensors that are used for finger recognition include optical sensors, thermal sensors, and capacitive sensors.

A recent patent in fingerprint sensing (US20140124583) relates to smart cards, which can be used as access control for entering the building, information display for bank cards and for security-related applications.

From 1994 to August 2014, approximately 5596 patents have been registered under smart cards. From 2008 to May 2014, approximately 124 smart card patents have been registered under biometric sensing. And approximately 104 smart card patents have been registered under finger print sensing. In 2014, the United States is the major patent holder for smart cards using fingerprint sensing. Fingerprint sensing will have a vast impact on the electronic security markets.

Fingerprint sensing is used in iPhone 5s smart phones to protect information and unlock the phone. Many smart phones in the future will have a fingerprint sensing application. Fingerprint recognition is a reliable and established technology. In the coming years, fingerprint recognition technology has opportunities to continue to be a dominant biometric authentication method, although in certain applications such as homeland security, fingerprint

identification will be combined with other technologies such as face recognition for more reliable probability of identification..

Biometric technologies, coupled with cloud computing, will open up new opportunities for growth. The biometric template database can be stored in the cloud, enabling low latency authentication programs.

Secure authentication processes are enabled with the help of biometric sensors. For attaining zero threat during transactions from mobile phones or smart cards, biometrics sensors are getting embedded in smart phones, debit and credit cards for safe and secure transaction. In the coming years, biometric sensors are expected to be deployed on visa cards, debit and credit cards of varied bank providers. Biometric technology is also expected to be coupled with cloud computing in the future. Thus, the recent trend suggests that both investors and inventors are focusing on deploying these sensors for authentication.

Title	Publication Date/Publication Number	Assignee	Inventor	Abstract
ADVANCED SMART CARDS WITH INTEGRATED ELECTRONICS IN BOTTOM LAYER INCLUDING BATTERIES, SWITCHES, DISPLAYS, AND FINGERPRINT SENSORS	08.05.2014; US20140124583	Reed Paul Stuart	Reed Paul Stuart	An advanced smart card comprising a top layer, a core layer of thermoset polymeric material, and a bottom layer comprising an Integrated Electronics Assembly. The Integrated Electronics Assembly may comprise a battery, a processor, a display, a switch, a magnetic stripe communications device, a flexible printed circuit, a fingerprint sensor, a biometric sensor, and an acoustic speaker. The advanced smart card may be used for functions such as: access control for building entry, data display for bank cards or ATM cards, password entry for identification cards, and fingerprint verification for security-related applications.
SECURE SMART CARD SYSTEM	20.02.2014; US20140052630	X-CARD HOLDING, LLC	Bona John Kenneth	A smart card usable in magnetic stripe swipe transactions with a transaction terminal configured to read transaction information encoded on a magnetic stripe of a standard transaction card includes a card body, which includes a magnetic stripe emulator for use with the transaction terminal, a smart card chip programmed with at least one transaction application for providing secured data for use in a transaction and dynamic card verification data, a power supply, and a card controller in communication with the magnetic stripe emulator. The card controller is configured to receive the dynamic card verification data and control the magnetic stripe emulator to emit a magnetic field encoded with at least a portion of the secured data and the dynamic card verification data.
SYSTEM AND METHOD FOR PROVIDING SMART ELECTRONIC WALLET AND RECONFIGURABLE TRANSACTION CARD THEREOF	20.02.2014; WO/2014/028565	RAO, Raj	RAO, Raj	A smart electronic wallet with reconfigurable multiple-account transaction card is provided. The system and method provide measures for storing a plurality of account identifiers from a plurality of traditional single-use transaction cards into a storage memory in a smart wallet. The system and method also provide for storing a reconfigurable multiple- account transaction card within the smart electronic wallet and allowing for it to be dynamically and selectively reconfigured for any one of the plurality of account identifiers stored within the smart electronic wallet. Additionally, a consumer is able to initiate a transfer or trade of transaction cards across different smart electronic wallet devices.

Title	Publication Date/Publication Number	Assignee	Inventor	Abstract
SMART CONNECT DEVICES FOR THE INTERCONNECTIVITY OF DATA CARDS WITH COMPUTING DEVICES TO ENABLE THE PERFORMANCE OF VARIOUS FUNCTIONS UPON AUTHENTICATION BY A USER'S FINGERPRINT AND/OR A USER'S PHOTOGRAPH	17.10.2013; WO/2013/155040	HENDRICK, Chaya, Coleena	HENDRICK, Chaya, Coleena	A connector device for connecting a computing device, mobile telephone or cellular telephone to a memory device, said connector device permitting the flow of data to and from said computing device, mobile telephone, or cellular telephone and to and from said memory device, with fingerprint scanning and verification on any combination of computing device, datacard, connecting device or wireless connectivity between datacard and computing device that may include combined fingerprint scanning and image capture and matching for secure authentication. Image capture may be done by image capturing capabilities built into a computing device combined with fingerprint scanning on the connecting device, datacard or computing device with the authentication process requiring combined matching of image/fingerprint.
Smart Hybrid Card System Providing Authenticity, Privacy, and Security (APS)	15.08.2013; US20130206837	Szu Harold	Szu Harold	An RFID/MFID system includes a tag and a reader. The tag is adapted to provide an RF identification signature when interrogated with an electric travelling wave and to provide an MF identification signature when interrogated with a magnetic travelling wave. The tag includes a target data object. The reader is adapted to read electrical and magnetic signatures of the target data object from the tag. A method of providing an identification function includes reading electrical and magnetic signatures of a target data object from tag. The tag provides an RF identification signature when interrogated with an electric travelling wave and provides an MF identification signature when interrogated with a magnetic travelling wave.
WIRELESS SMART CARD AND INTEGRATED PERSONAL AREA NETWORK, NEAR FIELD COMMUNICATION AND CONTACTLESS PAYMENT SYSTEM	18.04.2013; US20130092741	Loh Michael	Loh Michael	A wireless smart card having a personal area network transceiver, such as a Bluetooth transceiver, to couple the wireless smart card with a mobile communication device, and a near field communication (NFC) and radio-frequency identification (RFID) transceiver to couple the wireless smart card to a wireless transaction device, and a transponder with a secure element to allow secure communications between the mobile communication device with the wireless smart card and the wireless smart card and the wireless transaction device is described. The wireless smart card allows, for example, contactless payment through a Bluetooth-enabled mobile communication device without modification to the mobile communication device.
Biometric-enabled smart card	07.02.2013; US20130036463	Shashidhar Nagaraja	Shashidhar Nagaraja	A biometrics-enabled smart card for use in transactional or identity applications (e.g., credit cards and identity cards). The biometric smart card includes a substrate, a biometric sensor capable of reading biometric information through the substrate, and a microprocessor to process, store, and authenticate biometric information. The substrate has a Young's modulus of at least abut 50 GPa and a thickness of up to about 0.5 mm.

Exhibit 1 lists some of the patents related to fingerprint sensing and smart cards.

Picture Credit: Frost & Sullivan

Back to TOC