The invention relates to an active matrix display (113a; 113b) with a bending radius of 20 mm or more.

Fig. 5
Published: with international search report (Art. 21(3))
Active matrix display smart card

FIELD OF THE INVENTION

The present invention relates to active matrix display smart cards. More specifically, the invention relates to reusable active matrix display smart cards.

BACKGROUND

Design

A smart card may have the following generic characteristics:

- Dimensions similar to those of a credit card. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimetres (3.370 x 2.125 in). Another popular size is ID-000 which is nominally 25 by 15 millimetres (0.984 x 0.591 in) (commonly used in SIM cards). Both are 0.76 millimetres (0.030 in) thick.

- Contains a tamper-resistant security system (for example a secure cryptoprocessor and a secure file system) and provides security services (e.g., protects in-memory information).

- Managed by an administration system which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates.

- Communicates with external services via card-reading devices, such as ticket readers, ATMs, etc.

Traditional; smart cards can be divided into three types: contact smart cards, contactless smart cards and hybrid types of smart cards.

Contact smart cards

Contact smart cards have a contact area of approximately 1 square centimetre (0.16 sq in), comprising several gold-plated contact pads. These pads provide electrical connectivity when inserted into a reader which is used as a communications medium between the smart card and a host (e.g., a computer, a point of sale terminal) or a mobile telephone. Cards do not contain batteries; power is supplied by the card reader.

The ISO/IEC 7810 and ISO/IEC 7816 series of standards define:

- physical shape and characteristics
- electrical connector positions and shapes
- electrical characteristics
- communications protocols, including commands sent to and responses from the card
- basic functionality
Because the chips in financial cards are the same as those used in subscriber identity modules (SIMs) in mobile phones, programmed differently and embedded in a different piece of PVC, chip manufacturers are building to the more demanding GSM/3G standards. So, for example, although the EMV standard 1 allows a chip card to draw 50 mA from its terminal, cards are normally well below the telephone industry's 6 mA limit. This allows smaller and cheaper financial card terminals.

Communication protocols for contact smart cards include T=0 (character-level transmission protocol, defined in ISO/IEC 7816-3) and T=1 (block-level transmission protocol, defined in ISO/IEC 7816-3).

Contactless smart cards

A second card type is the contactless smart card, in which the card communicates with and is powered by the reader through RF induction technology (at data rates of 106-848 kbit/s). These cards require only proximity to an antenna to communicate. Like smart cards with contacts, contactless cards do not have an internal power source. Instead, they use an inductor to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics.

Hybrids

A hybrid smart card which clearly shows the antenna connected to the main chip. Dual-interface cards implement contactless and contact interfaces on a single card with some shared storage and processing. An example is Porto's multi-application transport card, called Andante, which uses a chip with both contact and contactless (ISO/IEC 14443 Type B) interfaces.

Applications

Below, an overview will be given of some important smart card applications as known nowadays. The present invention is applicable in all these fields, even though not restricted to them.

Financial

Smart cards serve as credit or ATM cards, fuel cards, mobile phone SIMs, authorization cards for pay television, household utility pre-payment cards, high-security identification and access-control cards, and public transport and public phone payment cards.

Smart cards may also be used as electronic wallets. The smart card chip can be "loaded" with funds to pay parking meters and vending machines or at various merchants. Cryptographic protocols protect the exchange of money between the smart card and the accepting machine. No connection to the issuing bank is necessary, so the holder of the card can use it even if not

---

1 The international payment brands MasterCard, Visa, and Europay agreed in 1993 to work together to develop the specifications for smart cards as either a debit or a credit card. The first version of the EMV
the owner. Examples are Proton, Geldkarte, Chipknip and Mon€o. The German Geldkarte is also used to validate customer age at vending machines for cigarettes.

These are the best known payment cards (classic plastic card):

- Visa: Visa Contactless, Quick VSDC, "qVSDC", Visa Wave, MSD, payWave
- MasterCard: PayPass Magstripe, PayPass MChip
- American Express: ExpressPay
- Discover: Zip

Roll-outs started in 2005 in USA. Asia and Europe followed in 2006. Contactless (non PIN) transactions cover a payment range of ~$5-50. There is an ISO/IEC 14443 PayPass implementation. Some, but not all PayPass implementations conform to EMV.

Non-EMV cards work like magnetic stripe cards. This is a typical USA card technology (PayPass Magstripe and VISA MSD). The cards do not hold/maintain the account balance. All payment passes without a PIN, usually in off-line mode. The security of such a transaction is no greater than with a magnetic stripe card transaction.

EMV cards have contact and contactless interfaces. They work as a normal EMV card via contact interface. Via contactless interface they work somewhat differently in that the card command sequence adopts contactless features such as low power and short transaction time.

Identification

A quickly growing application is in digital identification. In this application, the cards authenticate identity. The most common example employs public key infrastructure (PKI). The card stores an encrypted digital certificate issued from the PKI provider along with other relevant information. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC), and various identification cards used by many governments for their citizens. Combined with biometrics, cards can provide two- or three-factor authentication.

Smart cards are not always privacy-enhancing, because the subject carries possibly incriminating information on the card. Contactless smart cards that can be read from within a wallet or even a garment simplify authentication; however, there is concern over criminals accessing data from these cards.

Cryptographic smart cards are often used for single sign-on. Most advanced smart cards include specialized cryptographic hardware that uses algorithms such as RSA and DSA.

Today's cryptographic smart cards generate key pairs on board, to avoid the risk from having more than one copy of the key (since by design there usually isn't a way to extract private keys from a smart card). Such smart cards are mainly used for digital signature and secure identification.

The most common way to access cryptographic smart card functions on a computer is to use a vendor-provided PKCS#11 library (a cryptographic token interface Standard). On Microsoft Windows the CSP API is also supported.

system was released in 1994.
The most widely used cryptographic algorithms in smart cards (excluding the GSM so-called "crypto algorithm") are Triple DES and RSA. The key set is usually loaded (DES) or generated (RSA) on the card at the personalization stage.

Some of these smart cards are also made to support the NIST standard for Personal Identity Verification, FIPS 201.

The first smart card driver's license system in the world was implemented in 1987 in Turkey, which had a high level of road accidents and decided to develop and use digital tachograph devices on heavy vehicles, instead of the existing mechanical ones, to reduce speed violations.

A smart card driver's license system was, for instance, later issued in 1995 in Mendoza province of Argentina and in 1999 in Gujarath (India).

In 2002, the Estonian government started to issue smart cards named ID Kaart as primary identification for citizens to replace the usual passport in domestic and EU use. As of 2010 about 1 million smart cards have been issued (total population is about 1.3 million) and they are widely used in internet banking, buying public transport tickets, authorization on various websites etc.

Since 2009 the entire population of Spain and Belgium has an eID card that is used for identification. These cards contain two certificates: one for authentication and one for signature. This signature is legally enforceable. More and more services in these countries use eID for authorization.

After August 14, 2012, the ID card of Pakistan will be replaced by the Smart ID Card. The Smart Card is a third generation Chip-based identity document that is produced according to international standards and requirements. The card has over 36 physical security features and has the latest encryption codes making it the safest card in the world.

Smart cards are also beginning to be used in emergency situations. In 2004, The Smart Card Alliance issued a statement expressing the need to "to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification". In light of this, emergency response personnel have now begun to carry these cards so that they can be positively identified in emergency situations. WidePoint Corporation, a smart card provider to FEMA, produces cards that contain additional personal information, such as medical records and skill sets. Cards like these provide immediate access to information, which allows first responders to bypass organizational paperwork and focus more time on the emergency resolution.

Public transit

Smart cards and integrated ticketing have become widely used by public transit operators around the world. Card users may use their cards for other purposes than for transit, such as small purchases. Some operators offer points for usage, exchanged at retailers or for other benefits. Example include the Octopus Card used in Hong Kong, London's Oyster Card,
Dublin's Leap card, Quebec's OPUS card and San Francisco's Clipper card.

A highly successful use for smart cards within the UK is in concessionary travel schemes. Mandated by the Department for Transport, travel entitlements for elderly and disabled residents are administered by local authorities and passenger transport executives.

Smart cards (to the ITSO standard) have been issued as bus passes to qualifying residents; however these smart cards can instead now be used by elderly and disabled people who qualify for concessionary taxi travel. These schemes are part of an additional service offered by some local authorities as an alternative for residents unable to make use of their bus pass. One example is the "Smartcare go" scheme provided by Ecebs.

Computer security

The Mozilla Firefox web browser can use smart cards to store certificates for use in secure web browsing.

Some disk encryption systems, such as FreeOTFE, TrueCrypt and Microsoft Windows 7 BitLocker, can use smart cards to securely hold encryption keys, and also to add another layer of encryption to critical parts of the secured disk.

Smart cards are also used for single sign-on to log on to computers. Smart card support functionality has been added to Windows Live passports.

Schools

Smart cards are being provided to students at schools and colleges. Uses include:

- Tracking student attendance
- As an electronic purse, to pay for items at canteens, vending machines etc.
- Tracking and monitoring food choices at the canteen, to help the student maintain a healthy diet
- Tracking loans from the school library

Healthcare

Smart health cards can improve the security and privacy of patient information, provide a secure carrier for portable medical records, reduce health care fraud, support new processes for portable medical records, provide secure access to emergency medical information, enable compliance with government initiatives (e.g., organ donation) and mandates, and provide the platform to implement other applications as needed by the health care organization.

Other uses

Smart cards are widely used to protect digital television streams. VideoGuard is a specific example of how smart card security worked.

The Malaysian government uses smart identity cards carried by all citizens and resident non-citizens. The personal information inside the MYKAD card can be read using special APDU commands.
Since April 2009, Toppan Printing Company has manufactured reusable smart cards for
money transfer and made from paper instead of plastic.

Bag tags

Another important field of application is in bag tags. Since it is envisaged that the smart
card of the present invention will have broad application in this field, a more detailed
explanation of this field will be given first.

Bag tags, also known as baggage tags, baggage checks or luggage tickets, have
traditionally been used by bus, train and airline companies to route passenger luggage that is
checked on to the final destination.

Prior to the 1990s, airline bag tags consisted of a paper tag attached with a string. The
tag contained basic information that was written or printed on the paper tag, namely the
airline/carrier name, flight number, a 5, 6 or 10 digit code and the name of the airport of arrival.
These tags became obsolete as they offered little security and were easy to replicate.

Current bag tags include a bar code. These bag tags are printed using thermal or
barcode printers that print on an adhesive paper stock. This printed strip is then attached to the
luggage at check in. This allows for automated sorting of the bags to reduce the number of
misrouted, misplaced or delayed bags. Automated sorting of baggage using laser scanner
arrays, known as automatic tag readers, to read bar-coded bag tags is standard at major
airports.

For flights within the European Union, bag tags are issued with green edges.
Passengers are eligible to take these bags through a separate "Blue Channel" at Customs.

Bar codes cannot be automatically scanned without direct sight and undamaged print.
Forced by reading problems with poorly-printed, obscured, crumpled, scored or otherwise
damaged bar codes, some airlines have started using radio-frequency identification (RFID)
chips embedded in the existing tags. E.g. in the US, McCarran International Airport installed an
RFID system throughout the airport. Hong Kong International Airport has also installed an RFID
system. The International Air Transport Association (IATA) is trying to standardize RFID bag
tags. There is a somewhat higher probability of reading RFID 5 tags automatically. Physically,
however, RFID tags are not more robust than barcode tags.

The term license plate is the official term used by the IATA, the airlines, and the airports
for the 10-digit numeric code on a bag tag issued by a carrier or handling agent at check-in.
The license plate is printed on the carrier tag in bar code form and in human-readable form, as
defined in Resolution 740 in the IATA Passenger Services Conference Resolutions Manual
(published annually by IATA). Each digit in a license plate has a specific meaning. The license
plate is an index number linking a bag to a Baggage Sortation Message (BSM) sent by a
carrier's departure control system to an airport's baggage handling system. It is the message
that contains the flight details and passenger information, thus enabling an automated baggage
handling system to sort a bag automatically once it has scanned the bar code on the carrier
tag.
Besides the license plate number, the current bag tags also contain the name of airport
of arrival, departure time, IATA airport code of airport of arrival, airline code and flight number
and the name of the passenger identified with the baggage (last name, first name).

More than 1% of all baggage worldwide gets lost or mishandled each year. The cost to
rectify this comes down to € 70 per bag, plus the airline may lose passengers to another
competitor airline. This is a major problem that the industry is looking to solve. Most baggage
sortation and processing systems at airports worldwide are based on visual bag tag data and
1D barcodes printed on paper bag tags. The barcode scanners have to be "in line of sight" in
order to be able to "read" the 1D barcodes and get them on the right "track" for it to be loaded
on the correct baggage carts or ULD (Unit Loading Device) and onto the correct aircraft.

An important reason why baggage gets lost is that the barcode on the bag tag is badly
readable, e.g. due to low toner printing or tears or folds in the bag tag. Implementing RFID
technology and printed paper bag tags with an RFID (UHF) tag inside and/or permanent RFID
(UHF) bag tags could reduce the baggage loss, however the adoption of RFID has proven very
slow due to high implementation costs, at least 80 of the larger airports in the world being
required to start reaping the benefits of RFID. RFID tags only solving 10% to 20% of all lost
baggage depending on type of tag, no business case being available or hard to make, permanent RFID (UHF) tags being unsuitable for displaying bag tag information or barcodes,
permanent RFID (UHF) tags having very limited applicability as the "receiving" airport needs to
be equipped with RFID devices and airports do not change overnight to RFID, and printed
paper bag tags with or without RFID tag being a financial and environmental waste due to its
single use.

When travelling by air, hold baggage has to be checked. This is done today at the airport
using manned (staffed) check-in or dedicated baggage check-in counters. Implementing an
automated, unmanned, baggage check-in process can make tremendous cost savings and a
faster automated process will also increase the throughput per m² at an airport, improve the
flow at an airport and postpone airport expansion with ever increasing total number of
passengers per year.

Pilots with automated unmanned baggage check-in counters are known. Less staff is
found to be required, but the process is slow as passengers have to label their bags
themselves, which is something they are not used to do. In fact, on average the automated
baggage check-in process takes longer than the traditional manned baggage check-in (1 min 5
sec versus little under 1 min).

In the field of bag tags, therefore, there is a need for a solution that not only provides a
fast way of processing, like RFID HF (not RFID UHF), but also eliminates the baggage-labelling
process. Ideally such solution would be backward compatible with existing visual bag tag
readers.

SUMMARY OF THE INVENTION
The object of the invention is to provide an active matrix display smart card with graphical user interface that can advantageously be used in at least all applications mentioned above.

This object is achieved by a smart card as defined in claim 1.

Advantageous embodiments are claimed in dependent claims.

The flexibility of the smart card, together with the display enhances user friendliness. Nowadays credit / debit cards are easily damaged if not stored as flat as possible. This is inconvenient for many applications, such as the envisaged bag tag applications in air transport where bags (or other luggage) may not always be treated very carefully: luggage may be thrown by staff from place to another.

The presence of a user interface allows multiple applications to co-reside on a single smart card. This potentially has profound effects on the way smart cards are issued, as no one vendor 'owns' the card. It could mean end users buying cards and installing 'apps' on it, similar to the Apple model, rather than banks or transport authorities giving cards to customers.

**Benefits**

The benefits of smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contactless smart card can be programmed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card. For example, a smart card can be programmed to only allow a contactless transaction if it is also within range of another device like a uniquely paired mobile phone. This can significantly increase the security of the smart card.

Governments gain a significant enhancement to the provision of publicly funded services through the increased security offered by smart cards. These savings are passed onto society through a reduction in the necessary funding or enhanced public services.

Individuals gain increased security and convenience when using smart cards designed for interoperability between services. For example, consumers only need to replace one card if their wallet is lost or stolen. Additionally, the data storage available on a card could contain medical information that is critical in an emergency should the card holder allow access to this.

In an embodiment, the invention provides a dual-display reusable electronic bag tag that can wirelessly receive bag tag data via RFID (HF) or via other wireless means, that is backward compatible with visual bag tag data and barcode in-line-of-sight scanning and tracking technology, that is compatible with track & tracing technology and that is adaptive to fit other (emerging) wireless communication technology regardless of whether or not this requires a local power supply.
According to an embodiment of the invention an electronic bag tag is proposed that is
configured to display bag tag data received from a first external source. The electronic bag tag
comprises miniaturized electronics. The miniaturized electronics comprises a processor
configured to process the bag tag data to obtain processed bag tag data. The miniaturized
electronics further comprises a wireless communication interface that is communicatively
connected to the processor. The wireless communication interface is configured to receive the
bag tag data from the first external source. The miniaturized electronics further comprises a
non-volatile memory that is communicatively connected to the processor. The non-volatile
memory is configured to store the bag tag data and/or processed bag tag data. The
miniaturized electronics further comprises a first display and a second display. Each of the first
display and the second display is configured to display at least a part of the processed bag tag
data.

The electronic bag tag may also be called a smart tag or a smart label.

The processor and non-volatile memory can be integrated in a single integrated circuit,
possibly together with further components.

The bag tag data as received in the electronic bag tag is processed to make it suitable
for displaying on the first and second display. It is possible that the tag data or parts of the tag
data can be displayed without processing, in which case the processor simply processes the
tag data by storing it in the non-volatile memory.

For backward compatibility purposes the use of embedded active matrix displays is
preferred and would be most cost effective given the amount of data and barcodes that need to
be displayed on the displays.

The first display and second display typically have identical outputs, but it is possible that
the two displays output different parts of the processed bag tag data.

By using and integrating two, thin, flexible or inflexible displays in a programmable
flexible or inflexible tag, the electronic bag tag can advantageously be made to display all bag
tag data including e.g. horizontally and vertically positioned 1D and/or 2D barcodes on two
sides of the bag tag in conformance with IATA specifications as described in the IATA Baggage
Services Manual, making it backward compatible with visual bag tag data and barcode in-line-
of-sight scanning technology as used at airports worldwide. The electronic bag tag can
advantageously be integrated with e.g. a RFID UHF assembly to make it compatible with the
scanning and tracking & tracing technology as used in some airports. Advantageously, the
electronic bag tag is reprogrammable and can be wirelessly updated eliminating the baggage
labelling process and making the bag tag reusable.

Hereinafter, embodiments of the invention will be described in further detail. It should be
appreciated, however, that these embodiments may not be construed as limiting the scope of
protection for the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS
Aspects of the invention will be explained in greater detail by reference to exemplary embodiments of the invention shown in the drawings but not intended as limiting the scope of protection which is defined by the annexed claims and their technical equivalents. In the drawings:

Fig. 1 shows the components in the printed circuit board layer of a flexible electronic bag tag of an exemplary embodiment of the invention;

Fig. 2 shows a perspective view of the layers build-up of a flexible electronic bag tag of an exemplary embodiment of the invention;

Fig. 3a shows the front side of a flexible electronic bag tag of an exemplary embodiment of the invention;

Fig. 3b shows a perspective view of the backside of a flexible electronic bag tag of an exemplary embodiment of the invention;

Fig. 4a and Fig. 4b show templates displayed on an electronic bag tag of an exemplary embodiment of the invention;

Fig. 5 shows an example of an embodiment of the invention with a touch screen as user interface; and

Fig. 6 schematically shows a system according to an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF THE DRAWINGS

The smart card of the invention is an integral, one-piece flexible, non-disposable, one or more times programmable, passive (without battery/local power supply) or active (with battery/local power supply), reusable, "permanent" smart card. Miniaturized electronics in the smart card are embedded in a printed circuit board (PCB) layer with a highly adaptive system architecture. Depending on the configuration the miniaturized electronics comprise e.g. an embedded RFID/UHF and RFID/HF wireless communication interface, embedded power management module, embedded main controller integrated circuit including a microprocessor and non-volatile memory, embedded electronic circuitry, one or two embedded displays, an embedded display driver integrated circuit, and/or other optional embedded wireless communication interfaces.

Fig. 1 shows a detailed view of an flexible printed circuit board (PCB) 201 of a smart card of an exemplary embodiment of the invention (possible other layers are shown in figure 2). Fig. 1 shows a standard debit/credit card form factor that is compliant with ISO/IEC 7810 ID-1. Depending on industry and/or customer requirements this form factor and/or dimensions can be different. ISO/IEC 7810 ID-1 form factor dimensions are approximately 85.70 mm x 54 mm x 2.3 mm. Alternatively an ISO/IEC 7813 form factor in terms of card thickness is used, being approximately 0.8 mm.

The PCB 201 has one or more flexible displays 113a, 113b, e.g. based on TFT technology.

The following electronic components not requiring a local power supply are shown: RFID
HF antenna 103; integrated circuit with HF 13.56MHz ISO 14443 and/or ISO 15693 support
104; RFID UHF antenna 105; integrated circuit with UHF 860 t/m 960MHz EPC Gen2
integrated circuit ISO 18000-60 support 106; main power management module 107; optional
power management module 108 for the first display depending on display used; optional power
management module for an optional second display depending on display used; main card
controller integrated circuit 110; optional security controller integrated circuit 111; first display
113a with integrated display driver integrated circuit; and optional second display 113b with
integrated display driver integrated circuit on the other side of the PCB.

The following optional electronic components requiring a local power supply are shown:
GPS receiver integrated circuit or hybrid GNSS integrated circuit 112; GSM/GPRS multi band
modem integrated circuit 115; GSM/GRPS/GPS antenna 116; SIM on chip or E-SIM 117;
speaker 118; V motor 119; LED light 120; one or more buttons 121 for on/off switching the
transmitting function of GSM/GPRS, GPS, DASH7 or other (future) wireless communication
technologies that can cause interference; MEMS motion sensor(s) 122; digital and analog
123 for relays, digital sensors and analog sensors; miscellaneous component 124 such as an
additional (non-)volatile memory, e.g. flash memory, or another wireless communication
technology such as DASH7, Bluetooth Low Energy or Zigbee; power supply 125 in the form of
a thin flexible battery, a thin flexible rechargeable battery with or without energy harvesting from
ambient light (via a solar cell) and/or movement (via sensors), or a lithium ion rechargeable
battery; a power management system 126, and a power management system feeding main tag
controller integrated circuit with 5V, 3.3V or 1.8V 127.

Typically, the RFID UHF antenna has a high readability and is orientation insensitive due
to symmetry by design. The RFID UHF IC protocol preferably conforms to EPC Class 1 Gen 2,
which supports contactless interfaces conform ISO 18000-60 (869 MHz), FCC (915 MHz) and
ETSI (865 MHz).

The flexible smart card can be activated by proximity to an active reader. When the
smart card enters a reader’s RF field, the power management converts the induced
electromagnetic field to the DC voltage that powers the chip in the smart card controller, which
can include the integrated (dual) display controller.

In case the smart card main controller has an integrated (dual) display controller or two
separate display controllers, the integrated circuit is typically able to run multiple applications
and execute command sequences and overhead duties. The integrated dual display controller
or two separate display controllers is/are used for driving the two displays. The smart card main
controller runs a proprietary operating systems based on open platform technology such as
Java, proprietary firmware including driver software for driving displays and other components,
proprietary security software and/or proprietary software applications.

The security controller 111 can be used for secure private data storage and/or secure
data display. The security controller optionally supports proprietary security algorithms.
However, advantageously, the smart card contains a tamper-resistant security system, for
example a secure cryptoprocessor and a secure file system, which provides security services
such as protecting in-memory information. PKCS#11 library functions may also be used, as well as CSP API of Microsoft Windows, and cryptographic algorithms like Triple DES, DUKPT and RSA. A PKI system where the key set is loaded (DES) or generated (RSA) on the card at the personalization stage may also be used. Other options are possible too, like the NIST standard for Personal Identity Verification, FIPS 201.

In an exemplary embodiment the flexible display is a dual flexible active matrix display with the following characteristics, although it will be understood that the invention is not limited to this exemplary embodiment. The front and rear display size is 2.7”, but may be larger or smaller. In the front plane a polymer substrate with E-ink technology is used. In the back plane a polymer substrate with Active-Matrix array using EPLaR technology or similar can be used making the display flexible. The total thickness of each display is approximately 1 mm or thinner. The flexibility or bending radius is 20mm or larger. The resolution is approximately 200 DPI. The display has a wide viewing angle. The gray scale levels can be either 1 bit or 4 bit. Low cost manufacturing of bi-stable flexible displays can be achieved using existing high yielding LCD factory and EPLaR technology. The display ultimately has a low power consumption and an input voltage of approximately 3 Volts. The display comprises flexible connectors.

In an exemplary embodiment the non-volatile memory comprises 32, 128 or 512 bits for user memory, 128 or 496 bits for EPC memory and reserved memory. The data retention is typically 50 years and the cycle endurance is 100,000. Optionally it is possible to implement chipsets with more memory or to extend and/or stack memory.

The system design of the smart card allows adding additional components such as but not limited to: button(s) for navigation purposes, smart card controller such as Smart MX, Desfire, and etcetera.

A hole 114 can be punched or drilled in the printed circuit board layer 201 to enable attaching a baggage strap to the smart card for attaching the smart card to a piece of luggage.

Fig. 2 shows an example of the layers building-up a flexible smart card 200.

A first layer 280a on a first side of the flexible smart card 200 is a laminated or glued transparent (flexible) polymer based film.

A second layer 270a on the first side of the flexible smart card 200 is a laminated pre-printed flexible polymer based substrate or PVC substrate (or other polymer like polycarbonate (PC), polyphenyl delta-butylene (PdB) or polyester, and etcetera) which may come in any kind of color combination and contain graphics, logo’s, printed barcode, passenger name, credentials and other types of branding.

A flexible thin film printed circuit board layer 210, which is a flexible inlay, has a highly adaptive architecture that includes printed electronic components, as are explained above with reference to figure 1. For the printed electronics conductive copper, silver ink and/or conductive polymers can be used. A thin film PCB can be made with an electronic circuitry using flexible
conductive copper in combination with highly miniaturized integrated chips (integrated circuits) such that it will not jeopardize the flexible integrity of the thin film PCB. The display(s) has(have) a flexible frontplane and backplane.

A third layer 270b on the second side of the flexible smart card is a laminated pre-printed flexible polymer based substrate or PVC substrate (or other polymer like polycarbonate (PC), polyphenyl delta-butylene (PdB) or polyester, and etcetera) which may come in any kind of color combination and contain graphics, logo's, printed barcode, passenger name, credentials and other types of branding.

A fourth layer 280b on the second side of the flexible smart card is a laminated or glued transparent (flexible) polymer based film.

Fig. 3a and Fig. 3b show a front side (Fig. 3a) and back side (Fig. 3b) of a flexible smart card in an application as flexible electronic bag tag 200 in an exemplary embodiment of the invention. The electronic bag tag 200 has wireless communication capabilities and an embedded flexible display 23a, 23b on both the front side 21a and the rear side 21b of the tag 2. The front side 21a and backside 21b can be identical from a construction point of view, however the content on the displays 23a, 23b may differ. Instead of a wireless communication interface, physical contact pads may be used, like the ones shown in Fig. 5.

The displays 23a and 23b are typically used to display variable information such as e.g. the license plate number, place and date of issue, the final destination name, the final destination and/or transfer routing in IATA airport code, the airline code and/or flight number.

An information area 22a, 22b next to the display 23a, 23b can be used to print non-variable information, such as e.g. the name of the passenger (i.e. the owner of the electronic bag tag), a barcode with the name of the passenger and/or an identification code of the electronic bag tag encoded therein, advertorial information e.g. in the form of an airline logo, and etcetera. Alternatively or additionally the non-variable information can be displayed on the displays 23a and 23b.

The main controller integrated circuit 110 typically contains a proprietary Operating System (OS) and a proprietary software application embedded in the OS layer. The embedded software application receives, converts and processes data and stores the data and/or processed data in the designated non-volatile memory. The processed data can be formatted such that it can be presented together with a pre-loaded template on the one or two displays. Two examples of in memory pre-loaded templates 60a, 60b are shown in Fig. 4a and Fig. 4b, respectively. The data shown relates to the example of a bag tag suitable for air transport applications. The OS can contain the possibility to "post-load" software applications in the smart card's memory.

Fig. 5 shows a schematic example of a smart card according to the invention. The smart card 300 shown in Fig. 5 comprises two separate displays. A first display 304 is the display intended to show the data, e.g. the data as explained in detail above with reference to the air transport application. This display 304 is either an active or passive (matrix) display. In order to
improve the ease of use for end-users/operators the smart card 300 also has a second
display 306 which is a touch screen to be used as a user interface. The smart card's main
controller IC is then connected to this touch screen 306 and arranged to display "buttons" (or
"keys") or the like on the touch screen that can be operated by a user. Operation of these
"buttons" results in instructions received by the smart card's main controller IC. These
instructions are then processed by this controller possibly resulting in output data shown on the
display 304. The display 304 and the touch screen 306 are preferably arranged on the same
side of the smart card making it much easier to keep the smart card within the dimensions as
prescribed for smart cards with the size of a credit/debit card. The touch screen embodiment
may be combined with one or more physical buttons. Also, the smart card 300 may have a
further display on its other side (not visible in Fig. 5). The smart card's main controller IC can
also display other information on the touch screen 306.

The touch screen 306 (and possible physical, not shown buttons) can only be operated
by a user when the smart card receives power from an external source in the case of a battery-
less smart card. To enhance security, operation of the smart card may only be allowed by the
smart card controller IC and/or security controller after receiving a PIN-code from a user via the
touch screen (or physical buttons) or data as to another safe action on the touch screen, like
performing a certain sweep with a finger over the touch screen. Recognizing a fingerprint of a
finger of a user pushed against the touch screen may also be used by the smart card main
controller IC and/or the security controller to allow access to the functions of the smart card.
Such a fingerprint should then be pre-loaded in the smart card's memory to allow the smart
card controller IC and/or security controller to compare the fingerprint data as received from the
touch screen 306 with genuine fingerprint data.

As shown, the smart card 300 has a series of contact pads 302 to communicate with a
reader/writer, although also here a wireless communication arrangement, like the one shown in
Fig. 1, may be used instead.

Fig. 6 schematically shows a system in which the smart card of the invention can be
used. Fig. 6 shows smart card 200 and a reader/writer arrangement 600 arranged to read data
from and/or write data from the smart card 200. To that end the reader/writer arrangement 600
is equipped with an antenna 602 to communicate with the smart card 200 if it is equipped as a
wireless smart card. The reader/writer 600 also comprises a contact unit 604 arranged with
contact pins arranged to contact the contact pads, like contact pads 302, of a smart card 300
having such contact pads. The reader/writer 600 will have suitable processing equipment 606
with a processor and memory storing programs and data. The way such a reader/writer
arrangement operates is evident to a person skilled in the art and will not be explained in detail
here.

For fast transactions in e.g. electronic bag tag applications, bag tag data sent from a
back-end system to the electronic bag tag can be kept to a bare minimum. For this a method
can be used whereby a part of the bag tag data, the so-called "license plate" number, is
converted on the tag using IATA specified barcode font for 1D barcodes so that no barcode
The bag tag data format coming from the airline back-end system can be sent in ASCII format and wirelessly transferred to the tag. The ASCII data received by the tag's main controller integrated circuit 110 is then converted using an ASCII converter and then processed by the tag's application and a method that allows sending of only variable bag tag data by using specially designed, "pre-loaded" and stored templates on the tag's main controller integrated circuit's non-volatile memory.

The smart card can optionally be securely "paired" or "synced" with a smart phone, tablet or other smart card with wireless communication capabilities (like blue tooth) belonging to a certain passenger, to allow a fast and secure baggage check-in/drop-off process and whereby baggage claim information can be sent, stored and displayed on the smart phone, tablet or other smart card via the wireless communication interface.

The smart card can be made as a passive smart card, so without a local power supply, by using highly energy efficient displays that only require power when data needs to be refreshed and that do not need power to maintain data on the display. Such displays are known as "bi-stable" and can be found in for instance electrophoretic displays from for example Eink and Sipix. Preferably, in order to safe as much energy as possible, when the card's matrix display has changed state and received the new data, the power as received from of the external source will be cut off and the card can be taken out or away from the external reader/writer device. Such a change of state is, then, preferably monitored by the main card controller IC 110.

In a battery-less smart card the energy needed to transfer data to the card, convert, process and display the data can be provided by an external RFID HF and/or UHF reader connected to a power source, whereby power inducted by the RF field of the reader is picked up by the card's RFID HF or UHF antenna to activate the card's main controller and to perform the data transaction until data is presented on the one or two displays.

The smart card can also be made as an active (dual) display enabled RFID UHF card by embedding a local onboard power supply. The smart card can alternatively be made as an active card to support e.g. other wireless communication components such as DASH7, Bluetooth (Low Energy), GSM/GRPS including an E-SIM (SIM on a chip), GPS or GNSS hybrid, and etcetera, for the purpose of wireless receipt of data over a longer range and improved indoor and outdoor tracking & tracing of the smart card.

The smart card can include all sorts of (MEMS) sensors such as 3-axis accelerometer, 3-axis magnetic sensor, single dual or tri-axis gyroscope, pressure sensor including altitude, and etcetera.

The main functionalities of the smart card in its application as an electronic bag tag are: (wireless) receipt of bag tag data (function 1); processing, storage and displaying of bag tag data (function 2); display of bag tag data and compatibility with conventional airport systems and technology (function 3); and tracking & tracing in airport's baggage systems, indoors in general and outdoors (function 4).

Re function 1 and function 4, the electronic bag tag can wirelessly receive bag tag data
using the following HF and UHF RFID frequency bands. The 13.56 MHz (HF) band can be used using the ISO/IEC 14443 interface (includes Near Field Communication) and/or the ISO/IEC 15693 interface. The 860/960 MHz (UHF) band can be used using ISO/IEC 18000-6C, EPC Gen2 for electronic bag tags with segmented electrophoretic displays. UHF is used in several airports in the world and recommend by IATA. A non-battery operated electronic bag tag using these HF and UHF frequencies classifies as a passive tag.

Re function 1 and function 4, the electronic bag tag can be made to wirelessly receive bag tag information using the following UHF RFID frequency band. The 433 MHz (UHF) band can be used using ISO/IEC 18000-7 also known as DASH7. An electronic bag tag using these UHF frequencies requires a battery and classifies as an active tag.

Re function 1 and function 4, the electronic bag tag can be made to wirelessly receive bag tag information using the following alternative frequency bands. The 2450 and 5800 MHz band can be used for 802.11 WLAN, Bluetooth and Zigbee standards. An electronic bag tag using these frequencies requires a battery and classifies as an active tag.

Re function 1 and function 4, the electronic bag tag can be made to wirelessly receive bag tag information using mobile networks. E.g. GSM/GPRS can be used for sending ASCII data (or other data formats) from a back-end system to the electronic bag tag.

Re function 2, the tag is typically operated by an (proprietary) operating system (OS) installed on the electronic bag tag's embedded main controller and by a proprietary application embedded in the OS layer which may contain an ASCII converter, IATA specified barcode font(s) and specially designed pre-loaded templates.

In order to achieve fast wireless transactions, the amount of data that is to be sent to the electronic bag tag is preferably kept to a bare minimum. For this reason no images will be sent to the tag, although possible, but data in ASCII format or any other suitable format is sent to and processed on the electronic bag tag's main controller using an ASCII or other converter. Binary data can be used for bi-directional request/acknowledge and security purposes. 1D barcodes can be generated on the electronic bag tag's main controller by translating the so called "license plate" number derived from the received bag tag data, using barcode font "interleaved 2 of 5" as specified by IATA Baggage Services Manual. Several specially designed templates such as e.g. shown in Fig. 4a and Fig. 4b, which resemble pre-printed paper bag tags, can be pre-loaded and stored on the tag's main controller's non-volatile memory so that only variable bag tag data needs to be sent. Depending on the received bag tag information, the correct template is selected and displayed.

Bag tag data can be stored on the tag's main controller's non-volatile memory, e.g. including bag tag data for the current trip with up to 4 flight segments and bag tag data of up to at least 2 previous trips (up to 8 flight segments).

Re function 3, for backward compatibility purposes the use of embedded active matrix displays are preferred and would be the most cost effective given the amount of data and barcodes that need to be displayed on the one or two sides of the tag. However the electronic bag tag's system architecture can accommodate other types of displays such as segmented
displays and passive matrix displays or a combination thereof.

Using the electronic bag tag's stored templates 60a, 60b, the variable bag tag data and 1D barcodes are then pushed towards the one or two active matrix displays and presented such that the tag is compliant with IATA specifications for baggage labels as described in IATA's Baggage Services Manual.

Conform the same IATA specifications the tag also needs to be able to function as what's known as a "Shengen" baggage label. To achieve this, each display may have two small green bars 61 printed on top of the display's left and right side using green transparent ink to indicate a so-called "Shengen" baggage label, which can be switched to black by positioning black pixels exactly behind the green bars in order to indicate a regular baggage label.

Re function 1 and function 3, in business critical operational environments such as airport check-in and baggage check-in, the operational efficiencies are gained when devices carried by passengers are non-reliant on batteries. The (dual) display electronic bag tag is therefore extremely energy efficient and can operate without a local power supply (battery) and still maintain data on the one or two displays. A battery-less electronic bag tag can nonetheless be written to using an external RFID HF reading device as a power supply source. The electronic bag tag's power management module ensures that power derived by the electronic bag tag's embedded RFID HF interface from the RF field of an external RFID HF device, which is usually around 5V, is exactly regulated to the supply voltage required by the tag's main controller and the electronic bag tag's two integrated displays such that the electronic bag tag's main controller can receive and process data and present this data on both its displays. The battery-less operation of the electronic bag tag and the low energy efficient nature of the RFID HF interface requires energy efficient display technologies like electrophoretic, bi-stable displays or displays with similar technology that only require power when data needs to be refreshed on the display.

Re function 1 and function 3, the electronic bag tag's system architecture can accommodate all sorts of other wireless communication capabilities such as DASH7, Bluetooth (Low Energy), GSM/GPRS including an E-SIM (SIM on a chip, also known as U-SIM), UMTS, LTE, CDMA, CDMA2000, GPS or GNSS hybrid, etcetera, for the purpose of wireless receipt (long range) of bag tag data and tracking & tracing of the tag. All of which would require the tag to have an embedded battery or embedded rechargeable battery.

For example, with DASH7 technology embedded in the electronic bag tag, baggage fitted with this tag can be automatically checked-in upon nearing the airport terminal within a range of approximately 1km enhancing the airport's flow and throughput, and its accurate indoor tracking and tracing capabilities.

Also GSM/GPRS capabilities can be of interest as it would enable baggage check-in at home or wherever there is GSM coverage, gives the airline the ability to remotely access the tag and re-route baggage by sending new bag tag data to the tag, and enables global tracking & tracing of baggage both indoors and outdoors when fitted with GSM/GPRS with or without GPS or hybrid GNSS.
The battery-less electronic bag tag may be used in the following showcase. A passenger performs an on-airport baggage check-in. The passenger is identified via his boarding pass. A Passenger Name Record (PNR) is retrieved from the back-end system. The passenger is asked to put his "hold-luggage" with his RFID-based electronic bag tag fitted on the belt / weight scale. The passenger's baggage is weighed. Bag tag data is retrieved from the back-end system. Bag tag data is sent from the baggage check-in counter to the battery-less electronic bag tag via the RFID HF interface. In the electronic bag tag the bag tag data is processed, the RFID UHF chip is updated and the processed bag tag data is presented on the displays of the electronic bag tag. The passenger's PNR record is updated and a baggage claim tag is produced and provided to the passenger. The passenger's baggage is sent off to the baggage sortation systems for processing toward the correct aircraft on the platform. The passenger proceeds to security check and gate. The passenger's baggage is being processed, scanned and/or tracked in the airport's baggage systems by reading the 1D barcodes from the tag's displays and/or by reading the tag's RFID UHF.

The battery-powered electronic bag tag may be used in the following showcase. A passenger performs an off-airport passenger and baggage check-in from any Internet enabled desktop computer, laptop, tablet or mobile device. The Passenger Name Record (PNR) is retrieved from the back-end system. The passenger checks-in, his seat is assigned, and the number of hold luggage is confirmed or updated. The passenger boarding pass is provided and passenger's bag tag data is wirelessly sent from the back-end system to passenger battery-powered electronic bag tag via the tag's GSM/GPRS interface. The bag tag data is retrieved by, processed and displayed on the electronic bag tag. The passenger proceeds to the airport and towards the dedicated baggage drop-off counter with the electronic bag tag fitted on the luggage. The passenger is identified, hold luggage is put on the belt/scale and bag tag data is read wirelessly from the tag via the RFID HF interface. The baggage is weighed and the PNR record is updated. The passenger's baggage is sent off to the baggage sortation systems for processing toward the correct aircraft on the platform. Passenger proceeds to security check and gate. The passenger's baggage is being processed, scanned and/or tracked in the airport's baggage systems by reading the 1D barcodes from the tag's displays and/or by reading the tag's RFID UHF and/or by locating the bag via GSM/GPRS and/or GPS triangulation.

Summary

Now a summary will be given of features of an important example of the present invention. The active matrix display smart card as described can display alphanumeric characters as well as high resolution graphics such as, but not limited to, photos, 1D and 2D barcodes, icons, animations and movies.

Data can be updated/changed/put on the active matrix display smart card, possibly without an on-board power source (such as a battery) using solely power drawn from smart
card contact reader/writer devices or using the induced electromagnetic field from RFID/NFC reader/writer devices.

The active matrix display smart card can be fitted with an optional 'security controller' that allows data to be securely transmitted to the active matrix display and can't easily be tempered with.

The active matrix display smart card can be considered a small "all-in-one" Personal Computer fitted into a smart card. It may contain among others a fully integrated active matrix TFT display, display drivers, a microprocessor, an operating system, software applications and a graphical user interface, contact and/or contactless communication, an optimized power management and memory.

Possible active matrix display smart card products, battery-less or with battery, are as follows:

- **Battery-less Active Matrix Display Contactless Smart Card with Graphical User Interface:**
  - Active Matrix Display can be either black & white with gray scales or color
  - Card supports communication compliant with ISO/IEC 14443
  - Card dimensions are compliant with ISO/IEC 7810 ID-1
  - Card thickness will be ≥ 0,79 mm but ≤ 2,3 mm

- **Battery-less Active Matrix Display Contact Smart Card with Graphical User Interface:**
  - Active Matrix Display can be either black & white with gray scales or color
  - Card supports communication compliant with ISO/IEC 7816
  - Card dimensions are compliant with ISO/IEC 7810 ID-1
  - Card thickness is compliant with ISO/IEC 7813, which is 0,79 mm

- **Battery-less Active Matrix Display Dual Interface Smart Card with Graphical User Interface:**
  - Active Matrix Display can be either black & white with gray scales or color
  - Card supports communication compliant with ISO/IEC 7816 and ISO/IEC 14443
  - Card dimensions are compliant with ISO/IEC 7810 ID-1
  - Card thickness is compliant with ISO/IEC 7813, which is 0,79 mm

Operation of the active matrix display smart card:

**Contact version:**

When the active matrix display smart card is inserted in an active smart card reader/writer device, the DC voltage coming from the reader/writer device powers the chip in the main card controller.

After verification, the card's data and/or status will be read and a certain transaction can then be executed and data written to the card. Information that is to be displayed will be transmitted from the main card controller to the active matrix display via the optimized power
management, which will convert the DC voltage to the required voltage for the active matrix display. When the card's active matrix display has changed state and received the new data, the power will be cut off and the card can be taken out from the reader/writer device.

Contactless version:

The 'Battery-less Active Matrix Display Smart Card' is activated by contact with and/or by proximity to a contactless active RFID/NFC reader/writer device. When entering the reader/writer device's RF field, the card's power management converts the induced electromagnetic field to the DC voltage that powers the chip in the main card controller.

After verification, the card's data and/or status will be read and a certain transaction can then be executed and data written to the card. Information that is to be displayed will be transmitted from the main card controller to the active matrix display via the optimized power management, which will convert the DC voltage to the required voltage for the active matrix display. When the card's active matrix display has changed state and received the new data, the power will be cut off and the card can be taken away from the reader/writer device's RF field.

Examples of active matrix display smart card market applications:

- Aviation industry: frequent flyer card with visual ticket and/or boarding pass data
- Aviation industry: passenger card with visual ticket and/or boarding pass data
- Public transport industry: next generation public transport card with visual ticketing and stored value data
- Banking industry: next generation debit and/or credit card with visual transactions and balance data
- Loyalty industry: next generation loyalty card with visual loyalty points and/or (discount) vouchers
- Security Access industry: next generation security access card with biometric data, frequently updated visual photo ID and personal data

Hardware Components of the active matrix display smart card:

1. Card
2. Optional antenna for contactless communication
3. Power management
4. Main card controller with integrated display controller
5. Optional generic smart card controller
6. Optional security controller
7. Active matrix TFT display module
8. Optional additional memory

A more detailed explanation per component:

1. Card Dimensions
   - Card dimensions compliant with ISO/IEC 7810 ID-1: 85.70 mm x 54 mm
   - Card thickness compliant with ISO/IEC 7813: 0.79 mm or otherwise < 2.3 mm

2. Optional antenna for contactless communication
   - Antenna to support contactless communication compliant with ISO/IEC 14443-4, Type A, 13.56 MHz

3. Power Management
   - Converts the induced electromagnetic field from a contactless smart card reader/writer device into the required DC voltage that powers the chip in the main card controller
   - Manages the DC voltage from a contact smart card reader/writer device that powers the chip in the main card controller
   - Converts the DC voltage to the required DC voltage of the card's integrated Active Matrix display.

4. Main Card Controller with Integrated Display Controller and proprietary Operating System
   - Integrated Circuit that is able to run multiple applications and execute command sequences and overhead duties
   - Compliant with ISO/IEC 14443-4, Type A, 13.56 MHz and ISO/IEC 7816 communication interface
   - Integrated Display Controller for driving an electrophoretic bi-stable active matrix display
   - Proprietary Driver Software for driving displays, button(s) and other optional components
   - Proprietary Operating System software, software applications and security software

5. Optional Generic Smart Card Controller
   - Smart system architecture that allows the accommodation of the most commonly used microprocessors or smart card controllers such as, but not limited to, SmartMx and any Mifare variant which are compliant with ISO/IEC 14443-4, Type A, 13.56 MHz and ISO/IEC 7816 communication interface protocols.

6. Optional Security Controller
   - Security Controller for secure displaying of data on the active matrix display

7. Active Matrix TFT Display
• Display size: > 1.9"
• Display type: reflective electrophoretic, bi-stable
• Back plane: polymer substrate with Active-Matrix TFT array
• Viewing angle: < 180 degrees
• Black & white with gray scales or color
• Flexible

8. Optional additional memory
• Smart system architecture allows accommodation of additional flash memory.

It is to be understood that the invention is limited by the annexed claims and its technical equivalents only. In this document and in its claims, the verb "to comprise" and its conjugations are used in their non-limiting sense to mean that items following the word are included, without excluding items not specifically mentioned. In addition, reference to an element by the indefinite article "a" or "an" does not exclude the possibility that more than one of the element is present, unless the context clearly requires that there be one and only one of the elements. The indefinite article "a" or "an" thus usually means "at least one".
CLAIMS

1. A smart card (200; 300) that is configured to display data received from a first external source, the smart card comprising miniaturized electronics comprising:
   a processor (110) configured to process the to obtain processed data;
   a communication interface (103, 104, 105, 106; 302) communicatively connected to the processor and configured to receive the data from the first external source;
   a non-volatile memory communicatively connected to the processor and configured to store the data and/or processed data;
   a first display (113a; 304) configured to display at least a part of the processed data,
   the first display (113a; 304) being a flexible matrix display and the smart card being flexible with a bending radius of at least 20 mm.

2. The smart card according to claim 1, wherein the smart card has a second display arranged as a touch screen (306) connected to said processor (110).

3. The smart card according to claim 2, wherein the smart card is arranged to receive predetermined data via said touch screen, comprising at least one of a PIN-code from a user via the touch screen, fingerprint data of a finger pushed against the touch screen and a predetermined action performed on the touch screen by a user, and to allow operation of the smart card only in case it has received said predetermined data and checked its correctness.

4. The smart card according to claim 1, 2 or 3, wherein the smart card comprises the following layers:
   a first layer (280a) on a first side of the smart card (200), which may be a laminated or glued transparent flexible polymer based film,
   a second layer (270a) on the first side of the flexible smart card (200) which second layer (270a) may be one of a laminated pre-printed flexible polymer based substrate or PVC substrate, a polymer like polycarbonate (PC), polyphenyl delta-butylene (PdB) or polyester,
   a flexible thin film printed circuit board layer (210) comprising printed electronic components, such as conductive copper, silver ink and/or conductive polymers, an electronic circuitry comprising flexible conductive copper in combination with miniaturized integrated circuits, as well as said flexible matrix display, the second layer being located between the printed circuit board layer and the first layer,
   a third layer (270b) on a second side of the flexible smart card which may be one of a laminated pre-printed flexible polymer based substrate or PVC substrate, another polymer like polycarbonate (PC), polyphenyl delta-butylene (PdB) or polyester,
   a fourth layer (280b) on the second side of the flexible smart card which may be a laminated or glued transparent flexible polymer based film, the third layer being located between the printed circuit board layer and the fourth layer.
5. The smart card according to any of the claims 1-4, wherein the first display is a bi-stable display, wherein the communication interface comprises at least one of wireless technology and contact pads.

6. The smart card according to any of the claims 1-5, being either a battery-less or battery-comprising smart card.

7. The smart card according to claim 5, wherein the communication interface comprises at least one of a DASH7 \((124)\), Bluetooth \((124)\), GSM \((15,116)\), GPRS \((15,116)\), UMTS \((15,116)\), LTE \((15,116)\), CDMA \((15,116)\), CDMA2000 \((15,116)\), GPS \((14,116)\) and GNSS hybrid \((14,116)\) communication interface.

8. The smart card according to any one of the preceding claims, further comprising a sensor \((122)\) communicatively connected to the processor, wherein the sensor is at least one of a 3-axis accelerometer, 3-axis magnetic sensor, single-, dual- or tri-axis gyroscope or pressure sensor.

9. The smart card according to any one of the preceding claims, wherein the received data is in ASCII format, the processor is arranged to convert this ASCII data into said processed data, the non-volatile memory is preconfigured with one or more templates \((60a,60b)\) and wherein the processor is configured to select a template from the one or more templates for displaying the at least part of the processed data on the first display using the template.

10. The smart card according to any one of the preceding claims, wherein the electronics further comprising a security controller \((111)\), and wherein the communication interface is further configured to communicate only upon presenting a matching or paired external smart phone, tablet or external smart card which is used to authenticate the owner of the smart card using the external smart phone, tablet or smart card and the security controller.

11. Use of the smart card according to any one of the claims 1-10, wherein the smart card receives the data for displaying on the first display, and wherein at least one of the first display is scanned by an external scanner.

12. Use according of the smart card according to claim 11, wherein the position of the smart card is located by an external location device.

13. System comprising a reader/writing equipment and a smard card according to any of the claims 1-10.
Fig. 2
Fig. 6
## INTERNATIONAL SEARCH REPORT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>WO 2011/093780 AI (SCANDINAVIAN AI RINES SYSTEM DENMARK NORWAY SWEDEN [SE]; BYGDEN JOHAN) 4 August 2011 (2011-08-04) page 7 - page 12</td>
<td>1-13</td>
</tr>
<tr>
<td></td>
<td>US 7 845 569 BI (WARTHER RICHARD 0 [US] ET AL) 7 December 2010 (2010-12-07) col umn 5, line 50 - col umn 6, line 3</td>
<td>1,5-7 , 9-13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-/-</td>
</tr>
</tbody>
</table>

* Special categories of cited documents:

- **A** - document defining the general state of the art which is not considered to be of particular relevance
- **E** - earlier application or patent but published on or after the international filing date
- **L** - document which may throw doubts on priority claim(s) on which the application to which the international search is to be made is based
- **O** - document referring to an oral disclosure, use, exhibition or other means
- **P** - document published prior to the international filing date but later than the priority date claimed

- **T** - later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- **X** - document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- **Y** - document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- **Z** - document member of the same patent family

**Date of the actual completion of the international search**

12 December 2012

**Date of mailing of the international search report**

20/12/2012

**Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016**

**Authorized officer**

de Ronde, Jan

---

Form PCT/ISA/210 (second sheet) (April 2005)
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>wo 2012/152745 AI (EC SOLUTION GROUP B V [NL]; HARKES ERIK JAN [NL]) 15 November 2012 (2012-11-15) the whole document</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>US 2011/147461 AI (CHEN CHAO-CHIN [TW]) 23 June 2011 (2011-06-23) the whole document</td>
<td>1,5-7, 9-13</td>
</tr>
<tr>
<td>A</td>
<td>US 6 863 219 BI (JACOBSEN JEFFREY JAY [US] ET AL) 8 March 2005 (2005-03-08) the whole document</td>
<td>1</td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SE 1000074 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2011093780 A1</td>
</tr>
<tr>
<td>US 7845569 B1</td>
<td>07-12-2010</td>
<td>NONE</td>
</tr>
<tr>
<td>DE 102007039041 A1</td>
<td>19-02-2009</td>
<td>CN 101778725 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 102007039041 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2190677 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2010537226 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20100042612 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2009024409 A</td>
</tr>
<tr>
<td>WO 2008000764 A1</td>
<td>03-01-2008</td>
<td>CA 2655401 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CN 101479739 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE 102006030406 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2009541883 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20090026160 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2010066072 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2008000764 A</td>
</tr>
<tr>
<td>WO 2012152745 A1</td>
<td>15-11-2012</td>
<td>NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 4819958 B2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2011134290 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TW 201123117 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2011147461 A</td>
</tr>
<tr>
<td>JP 2003123047 A</td>
<td>25-04-2003</td>
<td>NONE</td>
</tr>
<tr>
<td>US 6863219 B1</td>
<td>08-03-2005</td>
<td>US 6863219 B1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 7417306 B1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2008315384 A</td>
</tr>
<tr>
<td>JP 2005285109 A</td>
<td>13-10-2005</td>
<td>CN 1926561 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2005285109 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KR 20070007134 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2007176622 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2012007096 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2005086088 A</td>
</tr>
</tbody>
</table>