WHITE PAPER

Secura Key
A Division of SOUNDCRAFT Inc.
Smart. Reliable. Secure.

TOPICS COVERED

- What is e*Tag®?
- Basic Operation
- e*Tag® Readers
- e*Tag® Credentials
- e*Tag® Card Memory Organization

Secura Key e*Tag® Technology

What is e*Tag®?

e*Tag® is Secura Key's brand name for its 13.56 MHz Contactless Smart Card Technology. e*Tag® cards, keytags, labels, readers and reader/writers using 13.56 MHz ISO 15693 technology are ideally suited for a wide variety of applications including access control, time and attendance, membership and loyalty programs, logical access, storage of biometric templates, parking and ePurse, fuel management, data retrieval, asset and inventory management, data collection and many others.

e*Tag® **readers** are designed to work with standard access control panels which provide an SIA Wiegand interface. When a factory programmed e*Tag® card is presented, the reader provides the panel with a facility code and card ID number in a standard Wiegand format. The panel provides feedback to the cardholder by using the reader's control lines to operate the red/green LED and audible beeper.

e*Tag® **reader/writers** and **Smart Readers** are designed to work with custom software applications developed by original equipment manufacturers and systems integrators. e*Tag® technology allows the host system to read and write to the card, and to store data on the card for one or more applications. The reader's beeper and LED can be operated by serial commands from the host.

This document is an overview intended to familiarize applications providers, consultants, resellers and end users with the capabilities of e*Tag®. To help implement new applications, Secura Key offers a software development kit and factory support.

Terminology

Technically speaking, an e*Tag® card or keytag is a High Frequency RFID Transponder. RFID stands for *Radio Frequency IDentification*. A *Transponder* is an automatic device that transmits a predetermined message in response to a predefined received signal.

In the non-access control market, for automatic identification and data collection applications, the term HF (High Frequency) RFID is used to describe e*Tag® technology. Although UHF (Ultra High Frequency) is the most common type of RFID technology for inventory and asset tracking, HF has advantages over UHF for certain applications, including less sensitivity to nearby liquids and the human body, as well as a much lower cost for reader/writers.

In the access control market, the term Contactless Smart Card is used to describe e*Tag® technology. This is because the original HF RFID chips were developed to replace "contact" smart card technology in transit and fare collection applications, and the word "contactless" was used to differentiate the new cards from traditional contact smart cards. When the cards were later used for security and access control, the terminology stuck.

Basic Operation

The e*Tag® card works in a similar manner to proximity cards: The reader/writer and the card both have an antenna tuned to the same frequency, 13.56MHz. The card is a passive device, which means that it has no battery.

The reader transmits RF energy at 13.56 MHz. When a card enters the reader's RF Field, that energy is magnetically coupled into the card's antenna, supplying power to the RFID chip in the card. The card transmits its serial number or UID (Universal IDentifier) to the reader by damping the reader's RF field in a pattern corresponding to the UID, which is factory-encoded into the chip. This causes a small ripple in the reader's RF circuit, which is demodulated and converted into data by the reader.

When the e*Tag® reader is in Wiegand/Auto Read mode (for access control applications) after it initially receives the UID from a newly presented card, it requests the first 5 blocks of data, where the Facility Code and ID Number are stored. If multiple tags are in the reader's RF Field, the reader communicates with the first tag read and ignores other tags. (An e*Tag® reader can also be configured to read and output the 64-bit UID in Wiegand/Auto Read mode.)

In Host Mode (for non-access control applications) the reader, controlled by an external program, may request data from various memory locations on the card, and may also write or rewrite data in various locations. When multiple tags are in the reader's RF field, the reader can make an inventory of all tags, it can read and write to individual tags, or it can write simultaneously to all tags.

Most Secura Key readers will power up in Wiegand/Auto Read Mode, unless they are configured for Host Mode. e*Tag® Reader/Writers can be switched into Host Mode by sending a command to the reader. Read-Only Models (containing RO in the model number) will only operate in Wiegand/Auto Read Mode.

ISO Standards

ISO (International Organization for Standardization) defines standard criteria for RFID or Contactless Smart Cards and Credit Cards. The ISO 15693 standard defines the RF protocol used to communicate between the card and reader, and specifies frequency, modulation depth and data rate.

The ISO 15693 standard allows a longer read range than ISO 14443[1] while still meeting FCC power output limits. The data transmission speed (baud rate) for ISO 14443 is faster than ISO 15693, but there is no noticeable difference in performance (better read range actually creates the perception of faster performance).

e*Tag® is an open standard ISO 15693 technology. e*Tag® readers can communicate with a wide variety open standard ISO 15693 transponders including TI HF-1, Philips iCode SLI, ST-Micro LRI, Infineon My-d and My-d Lite. Secura Key currently uses Texas Instruments HF-1 for the 2K-bit credentials, Infineon My-d (SRF 55V10p) for the 10K bit credentials, and ST-Micro 512 bit IC for the 512 bit adhesive tag.

[1] Many tags comply with ISO 14443, but the most widely used is NXP's MIFARE which uses ISO 14443A

Open Standard vs. Proprietary Technologies

e*Tag®'s interoperable, ISO 15693 open standard technology means that customers are not locked into a single-source for transponders or readers.

While other contactless smart card vendors meet the ISO 15693 or ISO14443 standards, this does not mean that their cards are open or interoperable with multiple vendors. The "secure" technologies require proprietary encryption algorithms and authentication keys to communicate with the card, and to access each individual sector. Each chip vendor, such as Philips (Mifare®) or Inside Technologies (Pico Tag® and HID ***iCLASS***®) has its own proprietary encryption algorithms, which are available under license or by purchasing a reader ASIC (Application Specific Integrated Circuit). Unless the reader has the required algorithms, it cannot read the stored data on the card; it can only read the UID (Card Serial Number). This means that if you choose a "secure" card technology, you are probably limited to one vendor for cards and readers.

With e*Tag®, data security is achieved by encrypting the application data, not by restricting access to the card. Because e*Tag® avoids the overhead associated with application directories and multiple sector authentication keys, the card reading process is much faster and simpler, and more card memory is available for applications. Open standard technology also makes the card much simpler to use for Application Providers. Application Providers are encouraged to implement their own unique data encryption to protect application data stored on the card.

Securing the Access Control Data

e*Tag® is frequently compared with MIFARE® by customers who require more security for Access Control data. Because of the complexity of managing authentication keys, many MIFARE® applications use the UID as the access control ID. This provides no security at all – the UID is unencrypted and can be read by any ISO 14443 reader. Additionally, the MIFARE® UID is 32-bits in length[2] , but is commonly truncated to 16 bits for access control with a synthesized facility code and parity bits, which can result in duplication of card numbers.

Secura Key never uses the UID for the access control ID number. Secura Key encrypts access control data, using modified DES encryption with diversified keys. Diversification uses the UID as part of the encryption key, which means that the encryption key is different for every card. If the bit stream is intercepted, a potential intruder cannot determine the actual access control data, and therefore cannot produce another card in the same series with the same facility code. Because the DES encryption key is diversified, data cannot be copied to a new card, because the new card will have a different UID, causing the decryption to fail, and the data would remain unreadable.

Secura Key readers decrypt the data and transmit it in Wiegand or hex formats. Secura Key's encryption methods and keys are not published, so that the security of the card data is protected.

[2] NXP's MIFARE® Ultralight and DESFire tags have a 56 bit UID.

e*Tag® Readers

e*Tag® readers and reader/writers are available in several form factors and colors. e*Tag® reader products can be classified in four groups: read-only models, read/write models, Smart Readers and OEM modules.

Read-Only Models (Wiegand Output)

ET8-RO-W-M – standard mullion housing - use on doorframes, mullions, limited space applications
ET8-RO-W-D-W and **ET8-RO-W-D-I** – Decora® style wall switch housing use on US j-boxes, wall surfaces
ET9-RO-W-MR – 6" x 6" housing - use on single or dual US J-boxes, wall surface

Fig. 1 Read-Only Models

These readers feature a standard Wiegand interface for use with most access control systems. They read Secura Key Wiegand format data which is factory-encoded on e*Tag® cards and key tags. The mullion reader is weatherproof and features a black housing with two LEDs. The Wallswitch reader is compatibly styled with the Leviton Decora® Wallswitch and is available in white or ivory. The high-intensity LED shines through the plastic housing.

The ET9 mid-range reader is weatherproof, and is designed for wall or post mounting. It is 6"H x 6"W, and has up to 8" of read range. In the future, this reader will be offered in read/write, PIN Keypad, and smart reader configurations.

Reader/Write Models

The e*Tag® reader/writers are available with a variety of communications capabilities. RS-232 units can connect to the serial COM port of a PC. RS-485 units can connect to a PC or microcontroller with an RS-485 port (or an RS-485-to-RS-232 converter) at distances up to 4000 feet. Up to 100 reader/writers can be individually addressed on one RS-485 network. For embedded applications, TTL communications can be used to link a reader/writer to a microprocessor. USB units communicate with PCs or other electronic devices with USB ports.

Fig. 2 Read/Write Models

Secura Key offers engineering support, protocol documentation and test programs for application developers.

The Read/Write Models are available in many different configurations. Most models with Serial Output (RS-232, USB, RS-485, or TTL also have a

Wiegand port, which can operate simultaneously with the serial port. The readers are available in Mini-Mullion or Wall switch configurations, and are fully epoxy potted for outdoor applications or exposure to water. Board-only versions can be embedded in other electronics to add RFID capability, and they are available with internal or external antennas. The model numbering scheme appears below:

ET4-XXX-XXX

Variables (X) from left to right

A – Auto Read (sends data immediately)
O – OEM (custom firmware, suffix after model number)
W – Wiegand (sends Wiegand format data immediately)
R – RS-232 output
U – USB output
X – RS-485 output
T – TTL Output
B – Board only with integral antenna
E – Board only, no antenna, embedded application
M – Mini-mullion housing (S-shaped)
S – Standard Wall switch housing
D – Desktop housing
-XXX – OEM Customer/version

Please contact Secura Key RFID Sales before ordering – not all variables can be combined.

USB Reader/Writers

The **USB Micro Reader** (ET9-USB-1) is a reader/writer with the same form factor as the popular USB memory stick – it is a small unit, which plugs directly into any USB port. It has an internal antenna with 2-3" read range, as well as an MMCX jack for an external 50-Ohm antenna, which can be switch selected. Secura Key offers a 1" x 4" antenna with a read range of 4-5". Secura Key can assist with custom antenna development. The unit is designed for special application providers, and a software development kit and factory support is available.

ET9-USB-1 ET4-AUS-D

Fig. 3 USB Reader/Writers

The **USB Desktop Reader/Writer** (ET4-AUS-D) is ideal for POS and enrollment applications. The low profile reader sits on a desk or counter and has non-skid rubber feet and a 6-foot long USB cable, and an internal antenna. The unit is designed for special application providers, and a software development kit and factory support is available.

Smart Readers

e*Tag® **Smart Readers** are designed to work with custom software applications developed by original equipment manufacturers and systems integrators. The readers communicate with the host via RS-485, and up to 100 units can be connected via RS-485 twisted pair to a PC or microcontroller for a host-validated system. The network can have a maximum length of 4000 feet. The reader has a solid-state relay, plus four inputs and two open collector outputs, allowing access control or process control without panels or additional hardware. Inputs and outputs can also be configured to interoperate under local control. Input circuits are capable of class B supervision. The host system can read from and write to the card over the RS485 network The host system also controls timed relay activation, LED and beeper activation.

Fig. 4 Smart Readers

The e*Tag® Smart Reader is available in two configurations: the ET8-SR-W-M (Mullion reader) used on doorframes, mullions, limited space applications; and the ET8-SR-W-D-W and ET8-SR-W-D-I, (Decorator reader) used on US J-boxes for interior applications.

Readers and Safety

e*Tag® readers meet FCC Class B standards for radiated emissions (approved for hospitals or residential use), and do not present a health hazard to the user. The readers do not emit full power all the time, but operate on a 20% duty cycle until they sense the presence of a card.

Power Supplies

e*Tag® readers require clean DC power for the best performance. A good, low-noise switching power supply will work. A noisy power supply may couple excessive RF noise into the reader, interfering with the card reading process, and resulting in very poor read range.

Readers and Performance Optimization

e*Tag® readers will work better if there is less metal nearby. Ferrous metal tends to absorb the RF radiation from the reader, leaving less energy to power the card, meaning that the card must be brought closer to the reader to operate. When mounted on a metal building or metal post-mount flange, a non-metallic spacer should be installed between the reader and the mounting surface to achieve the best read range.

e*Tag® Credentials

e*Tag® cards and tags offer 2K bits or 10K bits of user-controlled data storage, plus a 64-bit CSN / Unique ID number. Adhesive labels have 512 bits of data storage. If the credential is used for an a access control application, the Secura Key Wiegand format data is DES-encrypted using diversified keys, encoded, and locked in the first 5 blocks of the card. The cards are laser-engraved with the card ID and facility code. If the card is not used for access control, the entire card memory is available to the user.

e*Tag® contactless credentials are available in three form factors: ISO Cards, Key Tags, and Adhesive Labels.

Fig 5. e*Tag® Credentials

ETCI ISO Card - These white, glossy, laminated PVC cards meet CR80 and ISO 7810 standards for size and thickness, and can be printed on both sides, using a dye-sublimation or thermal transfer card printer, or they may be custom printed by the factory. See card printing guidelines in the Card Ordering Guide on the Secura Key website. They can also be slot punched for vertical (portrait) or horizontal (landscape) orientation. The access control ID number is laser engraved on the card. They are NOT embossable.

e*Tag® cards are also available with multiple technologies, allowing transition from (or use with) legacy systems, including magnetic stripe, Barium Ferrite, and Wiegand (see Product Guide). e*Tag® combined with Wiegand technology requires a thicker card (0.037" or 0.94mm). Matching encoding for multiple technologies is available – call factory for details. Secura Key does not encode magnetic stripe cards.

ETST Key Tag - These rugged 65 mil PVC key tags include a hole for use with most key rings. Custom printing is available. The access control ID number may be laser engraved on the tag.

ETKT Key Tag - These tags are similar to the ETST, except that they have a rounded end, and they are optionally available with an eyeleted hole for increased durability.

ETAT Adhesive Label - These thin, flat labels are 1.730" wide x 0.945" high and 0.014" thick, and have an industrial adhesive backing. They can be affixed to non-metallic surfaces of PDA's, cellular phones, briefcases, and other personal items or assets. They can also be affixed to the back of existing ID or Access Control cards using other technologies such as Proximity, Wiegand, Barium Ferrite, or Magstripe, allowing transition to e*Tag® technology without costly re-badging.

The labels may not be compatible with all insert, swipe or motorized tractor-feed readers – it is strongly recommended to request a sample label to test the desired application.

Cards and Safety

e*Tag® cards do not constantly transmit data, and do not present a health hazard to the user. The cards do not contain ferrous material, but if they have a metal spring clip or retractor, they should be removed when entering an MRI area. The cards should not be laundered, and should never be placed in a microwave oven.

e*Tag® cards contain an integrated circuit and an antenna. While they are fairly rugged and will last a long time if properly treated, they should not be bent back and forth, or subjected to strong impact, poked with a pencil, or otherwise abused. If the antenna is cut, broken or if the chip is cracked, the card will stop working.

Printing Cards

e*Tag® ISO (ETCI) cards can be printed in a dye sublimation printer. Card artwork designs should avoid areas of solid color or light screened patterns, as this tends to reveal the electronics embedded in the card. Make a test run of a new card printing design before printing all of your cards, and be prepared to make adjustments in the layout to avoid printing critical graphics in the area of the card chip. Dye Sublimation printing will not damage or warp the card if the printer is functioning properly. However, if a clear polyester overlay is applied, the heat used in many overlay laminators may cause the card to warp.

Cards should not be slot punched prior to dye sublimation printing, and should only be punched at the locations identified by a pre-printed slot punch target (a small "+"). Slot punching in other locations may damage the card's antenna, causing the card to stop working.

Card Encoding

e*Tag® access control cards are encoded with an ID number and facility code, which is used by the access control system to locate a cardholder record where access privileges are stored for each reader. Secura Key offers cards encoded with either 26-bit SIA or 32-bit Secura Key Wiegand formats. The Secura Key 32-bit format is recommended because it less widely used, and because it offers many more unique facility codes than 26 bit, reducing the possibility of duplicated cards. Secura Key can provide cards encoded with any OEM Wiegand format up to 40 bits – call the factory for information.

Hardware Interface

e*Tag® readers are equipped with an 18" unshielded 22AWG wire pigtail, with wire colors and functions shown in Table 1. Some models have a detachable cable assembly, while others are permanently connected to the reader. Board-only models provide solder pads with through-holes with the same connections.

Power

e*Tag® readers accept either a 5 or 12 VDC power supply, and can operate over a range of 5-14VDC. As with all RFID readers, noise on the DC input power will affect performance and read range, so a good quality DC supply should be used.

Power consumption (35-50 mA avg. / 65-90mA max) is about the same as Secura Key proximity readers.

Wiegand Connections

Wiegand connections are identical to Secura Key proximity readers, and they meet the SIA Wiegand standard, which has two lines for Wiegand data: Data 0 and Data 1. Cable from the reader to the panel should be limited to 500 feet.

LED, Beeper Connections

The Green LED and beeper will activate briefly to indicate a successful card read, otherwise the LED is normally off. The LED and beeper inputs are activated when asserted (grounded or held to logic low, below 2.5VDC)[3] and control cable from the reader to the panel should be limited to 500 feet.

[3] Model ET9 below 1.5VDC

Hold Input

The Hold Input is a control line which when asserted would buffer one card read until the line is released, at which time the last card read would be transmitted. This input can be connected to the contact or logic output of a vehicle loop detector, so that the card reader will not accept a card unless a vehicle is present.

READER CONNECTIONS					
Wire #	Wire Color	RS-485 Models	RS-232 Models	TTL Models	NOTES
1	BLACK	GROUND (-)	GROUND (-)	GROUND (-)	
2	RED	9-14 VDC (+)	9-14 VDC (+)	9-14 VDC (+)	
3	BLUE	HOLD LINE	HOLD LINE	HOLD LINE	Ground to Activate
4	YELLOW	BUZZER	BUZZER	BUZZER	Ground to Activate
5	BROWN	RED LED	RED LED	RED LED	Ground to Activate
6	ORANGE	GREEN LED	GREEN LED	GREEN LED	Ground to Activate
7	GRAY	RS-485 - A TXD	TXD	TXD	
8	VIOLET	RS-485 - B RXD	RXD	RXD	
9	WHITE	WIEGAND DATA 1	WIEGAND DATA 1	WIEGAND DATA 1	Open Collector Output
10	GREEN	WIEGAND DATA 0	WIEGAND DATA 0	WIEGAND DATA 0	Open Collector Output

Table 1 e*Tag® Wiring Connections

Serial Inputs

The ET4-WRx has serial RS-232 receive and transmit lines for connection to a host system. There are no handshaking lines provided. The host serial cable ground can be connected to the reader's power ground input. RS-232 cables should be limited to 100 feet from the reader to the PC or control panel.

The ET4-WXx and ET8-SR-X models have serial RS-485 receive and transmit lines for connection to a host system. Up to 100 reader/writers can be connected on the same bus, using Secura Key protocol. RS-485 cable from the host system to the last reader on the bus should be limited to 4000 feet.

Using e*Tag® for Non-Access Control Applications

To use e*Tag® Reader/Writers for non-access control applications such as biometrics, time and attendance, vending, etc., the Application Provider must write or adapt their application to use the e*Tag® protocol. Once this is done, the Application Provider will have an integrated offering consisting either of an e*Tag® reader connected to a PC or specialized terminal, or an e*Tag® OEM module embedded inside a specialized terminal, or a device such as a printer, fuel dispenser, photocopier, vending machine, etc.

The Application Provider will also develop software or some other means of programming their application data into e*Tag® cards, such as an enrollment station in the case of biometrics, a cash acceptor or credit card terminal in the case of cashless vending applications, or a software

program in the case of time and attendance applications. Most Application Providers can easily adapt their equipment to the e*Tag® Reader/Writers' RS-232 or USB interface.

The RS-485 interface is slightly more complex when multiple readers are used, requiring an addressing scheme and polling of connected readers by the host. ET4-WXx readers have a different RS485 protocol than ET8-SR Smart Readers.

The ET9-USB-1 USB Micro Reader SDK includes virtual COM port drivers for Windows XP and Vista, instructions, and an external antenna.

The ET4-AUS-D USB Desktop Reader is a USB Windows Human Interface Device, which does not need a driver, although the application software must be written specifically for this interface.

The e*Tag® Software Developer's Kit contains a protocol document, e*Tag® Host test software, and a reader. A Windows platform is not required to communicate with the e*Tag® reader – low level protocol commands can be used by microcontrollers and non-Windows software platforms. These applications can be written in C or Assembly language.

e*Tag® Card Memory Organization

Depending on the model of card ordered, e*Tag® cards might have either 2 Kbits or 10 Kbits of total memory. A 32 Kbit memory size is also available.

The 2K bit card has 64, 32-bit blocks, or 2048 bits of total User Memory. If the card is ordered for Access Control applications, Secura Key uses Blocks 0-5. The UID and administrative data is separate from User Memory (Figure 6).

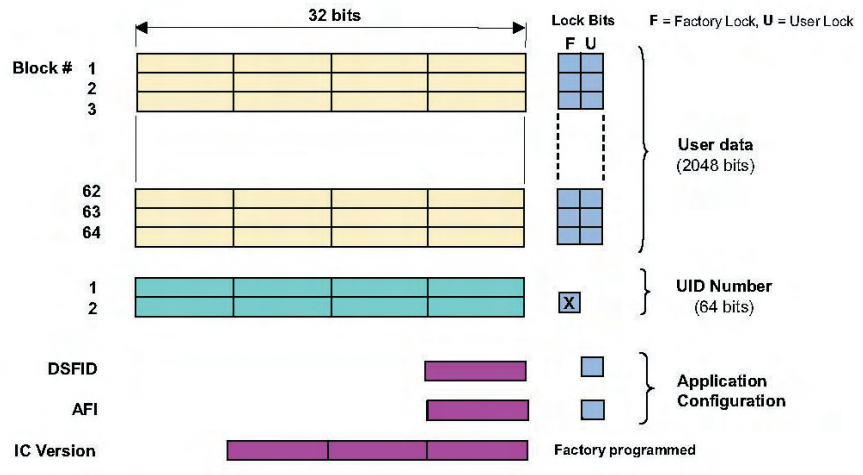

Figure 6. Memory Organization of the e*Tag® 2K Card

The 10K bit card has 248, 32-bit blocks, or 7936 bits of total User Memory. If the card is ordered for Access Control applications, Secura Key uses Blocks 0-5. The UID, and other administrative data consume 2304 bits of memory separate from the User Memory on the 10K bit card (Figure 7).

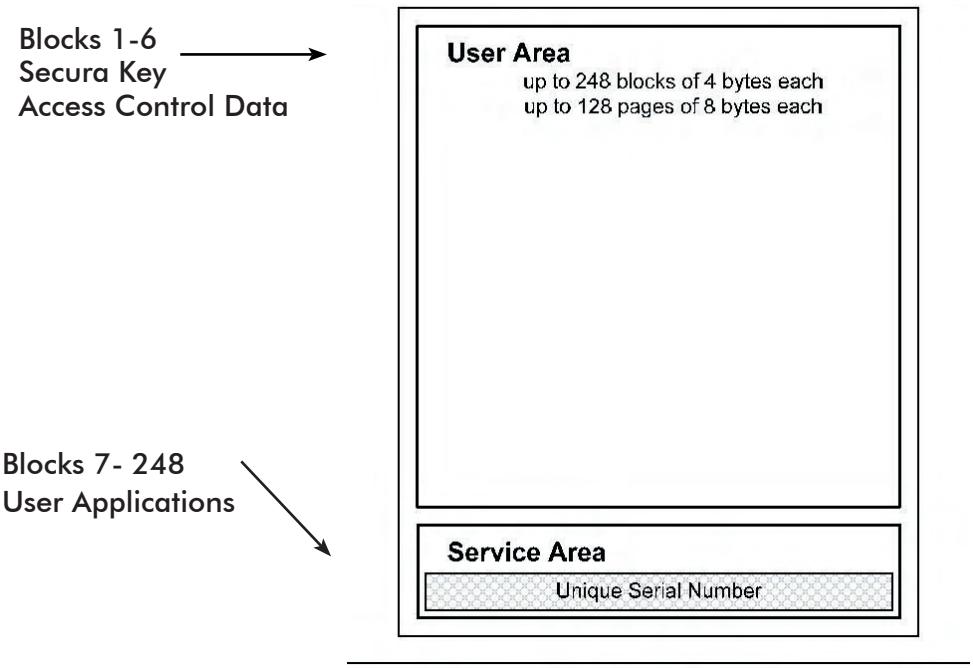

Fig. 7 Memory Organization of the e*Tag® 10KCard

Contact Info

Secura Key
20301 Nordhoff St.
Chatsworth, CA 91311
www.securakey.com