

Document Layout

This document is meant to serve as an introduction to our contact less smart cards. The goal of this document is to provide the necessary background detail for the reader in order to be able to answer potentially "interesting" questions by a journalist. The hope is that once the readers has perused through this document he/she shall have sufficient information and training to answer any further queries. We first detail the usage of smart cards in typical scenarios. It is important for the reader to familiarize himself with the current usage models of smart cards and understand how does our product differ from existing RFID or smart card technology. This is important to understand because many naive concerns people have are based on an unfamiliarity of the technical details of these technologies. We then outline the security details of our contact less smart cards and it is imperative that the reader understands this section well. Most potential questions are expected to be in the realm of security and the misuse of such technology. We also present a section that compares RFID technology with our product since this is another realm of potential concern. There is significant concern over the misuse of RFID or its lack of privacy that fuels speculation and significant business decisions. It is important for one to understand the differences and how is it that we offer addition security. Finally, we present a section that is devoted almost entirely to a few questions and answers on the material presented. The idea is to be able to assimilate this material and then use it to answer questions. We repeat important points/concerns in this document in an effort to drive home the point to the reader. Please treat such issues as potential questions on the interview.

What is our product?

We are selling a unique product that is a *secure* contact less smart card. It is born out of the synthesis of RFID's mobility features, the computable power of smart cards, cryptographic and biometric techniques for security. In our pilot programme, the aim is to deploy these cards as *stored value* cards in amusement parks in an effort to enhance consumer experience. Our cards will only function when used in extreme close proximity of a reader. The cards have very little memory capabilities and they do not store a history of transactions on them. An an effor to improve security, the owner's finger prints are read bio-metrically and then used to generate a unique signature that is used in all transactions. These stored value cards can be credited value at various kiosks around the park. These kiosks can also be used to check the balance/credit on a card.

Smart Card Usage

Currently smart cards using contact less technology have been utilized as stored value holders for many major metropolitan areas worldwide^[1]. Many of these cards are used mainly for mass transit; however, in some locations they are gaining significant ground as a form of electronic money. Hong Kong's Octopus card was launched for use in mass transit in 1997 and is today being used for other forms of transit such as car parking lots and meters, vending machines, retail purchasing including convenience stores and supermarkets, and more^[2]. Japan has a few such cards in place for the countries various mass transit and light rail systems, and Suica, the card used in Tokyo and the surrounding areas, has begun to be used for vending machine and station retail purchases as well. Both Octopus and Suica use Sony's FeliCa RFID technology^[3], which allows power to be induced from the reader and utilizes the computing power of the smart card's microprocessor to perform mutual authentication and provide for a much better level of security than most passive RFID systems. Adoption in these areas suggests that the trend towards electronic money by use of stored value smart cards will likely become attractive to other areas, particularly cities with the card infrastructure already in placed for mass transit.

Within an amusement park or resort, such a card could be used effectively for stored value electronic currency, access, and identification. Stored value would eliminate the need to fumble with currency and

speed check out times at POS terminals, and many hotel rooms use magnet strip access cards and the shift to contact less smart card would provide marginal convenience to the patron. A card could have age programmed in for things such as alcohol purchasing, allowing a patron to leave their wallet in their suitcase. Within an amusement park or resort the security risks for such a card should be further diminished. While utilizing such a system in a major city requires that cards be kept by individuals for long periods of times, the natural turn over of cards within a closed system such as a resort would make it possible to refresh information and programming such as encryption algorithms on a periodic basis to help prevent against fraud. Privacy concerns at a resort tend to be less significant than at home, patrons are staying in hotels not their houses, and are expecting more in terms of services. While a mass transit card allows an individual's movement over the course of a normal day to be monitored, patrons at a resort should be less worried about such information. It seems likely that someone on vacation would be willing to trade off the privacy of location data for the services that could come along with doing so – for example if a patron goes to the beach, the hotel provides fresh towels and more sunscreen upon their return. To further diminish privacy concerns, cards could have a reasonable opt out for patrons, such as carrying cash.

Security

Unlike the range of RFID chips, which are able to be read from long distances, contact less smart cards operate only up to approximately 10 centimeters. Contact less smart cards support many security features to ensure the integrity, confidentiality, and privacy of information stored or transmitted, which is possible because of the on-board microprocessor, a feature that is not available using traditional RFID tags. Security features on our smart cards include, but are not limited to, the following:

- Mutual authentication. A reader must perform a secure handshake with the smart card before the smart card securely sends encrypted data to the reader. This encrypted data helps to prevent eavesdropping, as cryptographically strong random number generators on the smart card can dynamically change keys, preventing third-party interception attacks.
- Smart cards are incredibly difficult to clone or forge because the chip manufacturers use computational scrambling encryption to secure data on the chip. Our smart cards are also resistant to physical tampering. During development of smart cards in the late 1990s, through case-by-case experimentation, data on a smart card could be erased or modified by an unusual power supply directly to the chip (cannot occur without someone stealing and dissecting one's smart card). However, because that is still a concern, our smart card chips have a variety of hardware and software capabilities, such as sensitivity to heating or UV lights, that detect and thwart possible tampering by third parties. Because these tampering techniques can only lead to a privacy breach if the card is stolen and the attacker successfully physically attacks the chip, our smart cards are considerably safer than identifying pieces of information such as drivers licenses or passports in their current forms. These attacks also are considered "class 3 attacks," which means that the costs associated to break the system are far more than the cost of the system itself.
- Smart cards only send a reader information that is authorized to view. Because the smart card does not send out any information to a reader that has not verified its credentials, smart cards do not just recklessly transmit. Information on a smart card is stored in a logical file system structure. At the top of each "file" (each piece of information) is a header that contains the access conditions for that file. Contact less smart cards can verify the authority of the reader and then only send out information that the reader is privileged to read. For example, personal information on a smart card could be protected further by requiring a PIN number or some other identifiable metric before sending out sensitive data. Thusly, smart cards actually help protect individual privacy by acting as a mediator between your data and readers that only releases information that the reader is authorized to access.
- Tight PIN security. PIN numbers on the card respond when the wrong PIN is entered several consecutive times. After that, the PIN is blocked and then requires a second PIN to unblock the data. The second PIN works in much the same way, except after several incorrect attempts, the card suffers from what is known as "irreversible blockage," and will not transmit any data. Some readers may even invalidate the entire card in this situation.

Encryption on our smart cards adheres to all Federal Information Processing Standards (FIPS), which are developed by the Computer Security Division within the National Institute of Science and Technology. The FIPS standards pertain to digital signatures, advanced encryption standards, and security requirements for the cryptographic model on the cards. Our smart cards generate verify signatures between itself and the reader using three different signature methods, including the powerful RSA digital signature algorithm.

RFID vs. Contact less smart cards

The main goal of producing contact less smart cards and smart cards in general, is to eliminate the use of the magnetic stripe technology. This new technology also increases security and privacy with its powerful embedded capabilities. Apparently data on the magnetic stripe can easily be read, written, deleted or changed with off-the-shelf equipment. Therefore, the magnetic stripe is really not the best place to store sensitive information. Extensive mainframe-based computer networks have been invested for verification and processing. But now with smart cards, the card carries the intelligence. With this in mind, other technologies have been evolving such as the RFID technology that presumes to ensure security and privacy. But there are some critical points of comparison that should be addressed between the two technologies.

There are three main reasons why smart cards are considered to provide more privacy protection and security:

- RFID technologies that are mostly used nowadays operate over long ranges (e.g., 25 feet), and have minimal built-in support for security and privacy, also increasing the chance of “skimming” any information on the RFID tags. Contact less smart cards, on the other hand, operate at a short range (about 10 cm), which in itself is more secure, and can support the equivalent security capabilities of a contact smart card chip which is more efficient than RFID provides.
- Contact less smart cards can perform efficient functions such as encryption and mutual authentication and interact intelligently through contactless readers. Moreover, contactless smart cards and readers can implement a variety of industry-standard cryptographic protocols (e.g., AES, 3DES, RSA, ECC) while RFID tags have had a hard time implementing sophisticated cryptography. Although it has been reported that RFID has embedded robust cryptography, experiments have found several vulnerabilities in several RFID systems examined. By reverse engineering the protocol between the cards and the readers, inexpensive RFID devices that emulate both cards and readers were constructed. This experiment points out that RFID cards are susceptible to disclosure of personal information and thus do not ensure data security nor individual privacy.
- Smart card technology has the ability to protect individual privacy. Unlike RFID technologies, smart card-based devices can implement a personal firewall for an individual, releasing only the information required and only when it is required.

Predicted Q&A

These are a subset of the questions one can conceive a reporter addressing. Please treat this as a "quiz" on the aforementioned material.

Q. Tell us briefly, what is a smart card? What is the product you're selling?

A. A smart card is a small (often pocket-sized) card that contains a microprocessor. Such cards are intended to provide transactional computability with secure transactions. Our products add radio frequency identification tags to smart cards. Hence our cards are contact less and free the consumer of the burden of having to carry any money or sign any papers thus making every transaction quick and easy. Our pilot program involves using these smart cards as debit cards in amusement parks.

Q. There has been considerable concern about RFID tags and privacy. What can you tell us about RFID?

A. RFID or Radio Frequency Identification Tag is a new piece of technology that involves a small tag that sends out signals that can uniquely identify the tag. RFID tags are very useful and are being increasingly considered for wide adoption to improve warehouse distribution and consumer experiences at various locations such as stores, supermarkets, malls, etc. RFID tags possess very little computational power as well as memory. However RFID tags are inherently not capable of providing security or authentication of any form.

Q. Is your product different from RFID? How does your product/technology tackle the potential pitfalls of RFID? For example, various groups have raised concerns about security, theft of data, identity impersonation etc. via the misuse of the technology. How would you respond to these concerns?

A. Our products combine the security features of smart cards with the mobility and ease features of RFID tags to create a contact less card. In other words we're combining the ying and the yang of this technology. As I pointed out earlier, RFID tags have very little processing power and hence provide very little security features. They are easy to activate and can function passively without any knowledge of whom they're interacting with. Our products on the other hand can authenticate themselves and each other before any transaction takes place. Our devices use state of the art cryptographic and biometric techniques to ensure that the device they're talking to is indeed what it claims to be. They also ensure that only the card owner can activate and use the card via biometric techniques. (Read the technical section for further details and be prepared to answer technical questions).

Q. Why do you envision the need for such contact less smart cards in an amusement park?

A. We believe consumers want to be free of all hassles in amusement parks (signing receipts, carrying cash, long lines, etc.). The focus is to increase the time consumers spend on actual rides and entertainment as opposed to carrying out transactions and this is where we come in.

Q. Will the technology increase consumer costs?

A. No, in fact this is intended to decrease operating costs at the park which in turn should lead to a decrease in prices for consumers. Additionally, we want to free the consumers of the responsibility of carrying cash and signing for every transaction within the amusement park.

Q. It seems like your trying to entice consumers to buy more and spend more money.

A. Our intention is making the consumer experience as pleasant as possible. If this encourages you to buy more than we are no more to blame than the internet which lets you order books, supplies and pretty much anything from your desk at home.

Q. Are smart cards a high price to pay for privacy? Do your products provide additional privacy?

A. No, they are not a high price to pay for privacy. Security and privacy have been our utmost concerns and we're using technology to address these issues. In fact our smart contact less cards provide the following security and privacy capabilities:

Support for biometric authentication: Only the owner of the card will be able to operate these cards.

Strong contactless device security: The microprocessors are hard to break into and are manufactured with features such as extra metal layers, sensors to detect thermal and UV light attacks, and additional software and hardware circuitry to thwart differential power analysis.

Mutual authentication: Cards will only be able to talk to those readers that provide proper credentials. To ensure the flow of information is not susceptible to attacks our powerful chips are using strong cryptographic techniques such as SHA-1 and RSA. These are the same techniques used for all other transactions on the internet.

Information privacy: These chips are memory-less in that they do not store transactional history.

If you really think about it, we're proposing to making the system a lot safer than any system that is actively in used today.

Q. What about data theft? Does this make it easier for somebody to learn of my transactions in the park?

A. I understand this concern but let me assure you that the technology in our microprocessors is such that all transactions are bio-metrically authenticated. Hence only if you touch the card will a transaction take place. Plus the cards do no store a history of the transactions and hence there is no opportunity for data theft or anybody learning of your transactions. The only way somebody can learn of your transactional history is via credit card statements.

Q. What about tracking user location in the parks?

A. This is left entirely up to the park authorities. Various parks are already using RFID to track lost children, families and groups. Its not the case that we're introducing technologies to make this easier. We are not in the business of tracking user locations and this is a policy that each park has to set for itself.

Q. Are there any potential mis-uses of the technology you are rolling out?

A. Any technology be it a computer or a heart monitor *can* be misused for purposes they were not intended to be used for. Therefore it is incorrect to speculate such questions, If the technology is rolled out, maintained, actively tested and upgraded in a timely fashion potential misuses can be avoided.

Q. Are you introducing any safe guards to prevent the amusement park from mis-using the system?

A. First of all, all transactions involve the biometric impression of the owner (who is required to touch the card) which generates a unique signature used in transactions and authentication. Therefore the transaction is secure and the "park" has very little role to play in the entire process other than provide a reader. This is akin to using credit card readers. Second, we have a system of accountability whereby consumers can flash their cards at various kiosks to either add value or check current balance. This helps them keep track of their balance.

Q. Do you envision your product being used in scenarios other than amusement parks?

A. Our initial product is meant for amusement parks. Our product cycle plan does potentially consider other uses such as resorts, malls, subways, buses etc.

[1] See http://en.wikipedia.org/wiki/Smart_card#Contactless_Smart_Card for a list of many of these cities.

[2] http://en.wikipedia.org/wiki/Octopus_card

[3] <http://en.wikipedia.org/wiki/FeliCa>