FTC Public Workshop on RFID

RFID Technology is not new. In the 1980's, Honeywell sold 40M units for tracking salmon migration in the Snake River. It was a 40bit ROM device with a unique ID number for each salmon. Since that time, much progress and refinement has been made in this technology and as it develops we will see much more of these devices as the price continues to fall. Today, contactless smart cards, tags and labels applications are becoming more widespread because they are easy for customers to use and fill a niche in the industry.

How RF works?

RF devices use two different means of transmission, depending upon the frequency used in the project. For low and high frequencies (125KHz and 13.56MHz), the RF transmission is through an electromagnetic wave. The antenna of the reader/writer and the one connected to the device act like a transformer and the electromagnetic energy if transferred from one antenna to the other, carrying power and signal. For the UHF (ePC, 915MHz), the transmission is through an electric field and reader/writer on one hand and the device on the other are acting like radio transmitters. Characteristics of transmission (data rate, distance of reading/writing...) are specific to each frequency. Each technology has its own intrinsic advantages and disadvantages and should be selected based upon the specific requirements of each project. No one technology has all the advantages. In general, the longer the reading/writing distance, the slower the data rate is.

Advantages of RFID:

They are many advantages of RFID. In transport (bus, train, subway) when there is heavy usage, a prepaid contactless card is often the easiest and quickest way for regular customers to pay for the fare. In banking and e-purse related applications, people like how easy it is to use – that they do not having to remove the card from the billfold to pay for their purchase. In an industrial environment, a tag or a label can be attached to a box or a piece part and the full history of the unit can be discovered instantly by reading the tag.

All of these applications are new to these industries and will expand exponentially in the future. In addition, the cost of technology continues to decrease every year as new materials are found and discoveries are made which will make it more attractive and fordable for industry.

Security and Privacy:

The issue of security and privacy differs between an ID card and a can of peas. For a can of food that currently uses a bar code, it is not necessary to pay extra to ensure increased security or privacy. In this case, an electronic tag that can be read at 4 meters for inventory control is a great tool. Nobody will try to tamper with this data and security or privacy is not an issue. However, in the case of an ID card security and privacy does

become a serious issue. To ensure both security and privacy, data encryption is a must. If data (demographic or biometric) is encrypted with a secure algorithm, it will be almost impossible for someone who is not authorized to read the data and/or tamper with it. For ultimate privacy, biometrics should be stored in the card itself and not in a database because it is to tamper with a database and software on a hard disc than it is to tamper with a piece of hardware.

Example of specific RFID technology –as potential solution to privacy problem:

One example of how RFID technology can help solve the privacy and security problem through the use of Crypto RF devices, which Atmel manufactures. These types of RF technologies can protect privacy and prevent the counterfeiting of products in the market place. These devices are able to solve the privacy and security aspects in the following ways: the concerns regarding privacy can be addressed, because the dialogue between the device and the host processor (or the application) is fully encrypted in the Atmel products. Information is kept secret and only authorized entities that know the secret keys can have access to the information. In terms of security, information residing in the device memory is encrypted with a 64-bit "rolling" key. Every time the device is powered by a request for information, the 64-bit key is different, using a random number generator. This means that, the message is always the same but looks different at each interrogation. A hacker looking at the same message several times will find "different encrypted messages" without relation. The content of the message remains the same for an authorized entity.

Furthermore, these types of devices are also ideal to fight fraud for many products pharmaceuticals, chemicals and cosmetic products. Such a device programmed by the manufacturer and then by authorized distributors along the supply chain, will prove to be authentic when it arrives on the store shelf.

In our e-mail we have attached a power point presentation. This document goes into more detail as to how one can use crypto RF technology to provide additional security and thereby protect the privacy of the information contained in the RF device. Furthermore, it sets forth the manner in which the encryption solution operates in the context of this RFID technology.