Using Secure Optically Variable Devices to Enhance the Security of RFID Identification Cards

Authors: Victor Zazzu & Wenyu Han ZBA Inc.

The use of RFID technology for Identification cards is becoming a common place occurrence. More and more information can be kept on the RFID cards regarding both the personal and/or medical data. This data can range from a several tens of bytes to tens of kilobytes, especially if biometric data is stored such as a facial photograph or an image of a fingerprint scan, or an Iris scan, etc. This information along with other items such as SS # is fertile ground for those who are in the identity theft business.

While most cards are password protected and/or encrypted there are brute force methods that can be used to defeat the encryption. The Johns Hopkins lab found that the code could be broken with what security geeks call a "brute-force attack," in which a special computer known as a cracker is used to try thousands of password combinations per second until it hits on the right one (1). More complex encryption algorithms will also make the hacker's job much more difficult.

One major issue that is always a concern in any Security system as related to RFID identification cards is the cost of the cards and readers. The use of a simple index look-up RFID inlay, will probably add approximately 50 cents to the retail cost of the card vs. just a plain printed card with a barcode or magnetic stripe. To further enhance the security of the card via the use of a smart chip the price of the card can increases to several dollars. Of course, as with any electronic items, the overall production quantity is a major factor in the determination of the final cost of the identification card.

While this article is focused specifically on RFID card security, if it's not obvious, the reader should be aware that the discussion applies to counterfeiting in general. The counterfeited items at risk include passports, drivers' licenses and other documents as well as labels for containers, pallets, boxes and individual product packaging.

Layers of security

A widely used method employed to enhance the security of any document such as an ID card or passport is to implement an ever "increasingly difficult to defeat" series of layers of security before the final set of usable data can be obtained. ZBA Inc. has done research and development (and patented) on a design flow and method of manufacturing of a secure RFID card system that is for all intents and purposes is impossible to defeat. The underlying idea is that since it is impossible to completely eliminate counterfeiting or identity theft you need to make your system so difficult to defeat that the counterfeiters will simply divert their attention away from your product and focus their efforts elsewhere. The foundation of this system design, herein after referred to as the "Eclipse system" uses a

series of unrelated physical structures located on the card to make each card unique and then subsequently use those characteristics to generate the encryption keys to encrypt the real data.

The Eclipse reader is then specially designed to read the physical Eclipse code and in combination with the data stored in the RFID card make a determination if the card is an original or a counterfeit. If the validation process returns a positive result then the reading of the cards encrypted data is then shifted to the next step in the reading process.

Details of the Eclipse Code

Many methods are used to try to make ID card or a document secure from Counterfeiting, or Genufeiting, and or Modeifeiting. (See appendix A for a glossary of terms). Many Secure ID card producers use a combination of covert and non-covert items including special difficult to obtain materials and or material combinations to produce an ID cards or document that have unique properties that will deter duplicators. Some of the item that are used are; a)energy converting inks b)micro and nano-printing, c) hidden or latent images, d)planned or specific defects, e)Holograms, and of course, f) a variety of encryption algorithms such as Triple DES or RSA. The major drawback to these systems is that that there is typically no correlation between the covert inks or nano-printing etc., and the RFID data.

This method embodied in the "Eclipse system" addresses each of these issues with an elegant design that is seamless and easy to manufacturer, but essentially impossible to duplicate while yielding an ID card that is unique. The manufacturer of the card uses an existing manufacturing flow with existing machinery. In fact the design of the process calls for very loose tolerances on certain aspects of the manufacturing process. Inherent in the design is a method that prevents the Original Card Manufacturer from generating a counterfeit second card (even if a rogue employee has access to all of the original documents and equipment). In many cases the following listing of items and description of the Eclipse system would be a closely guarded secret but in this case even knowing the specific details of the operation of the system will not provide a counterfeiter the ability to generate counterfeit cards. The Eclipse codes may be formed in several different ways, but in this example we are using a security Hologram as the carrier of the Eclipse code.

Eclipse Card Process Flow

The process starts with the choice of the materials and the cards design. The first item is to design the artwork of card and choose the appropriate location of the human readable identification information, the location of a photo or image of the fingerprint, and the location of the security Hologram and the design of the C-thru (HRI) protective overlay.

A portion of the Eclipse code is formed as part of the Hologram design, an additional but completely independent process step is performed to form the second part of the Eclipse code. The following

images are examples of a Hologram design that includes a proprietary machine readable code. For obvious reasons the description of the machine readable portion of the Hologram is not disclosed here. Additionally, there are additional embedded forensic items that can be used for laboratory analysis. These items are not the scope of this paper and will not be discussed here. Figure 1 shows the Hologram design in which the following sets of drawing contains the artwork with a significant amount of information of which only a certain portions of the information is capable of being read by a specially designed optical detector. The balance of the optical information from the Hologram is purely diversionary. The hologram is designed with hot stamping adhesive and is stamped onto the cards surface without any means of image to card surface registration. This factor is used to our advantage to form the Eclipse code.

The next item is to choose is the design of the protective overlay. Hologram material is constructed of an extremely thin layer of aluminum deposited onto an embossed Polyester film. The hologram material is subject to scratching and physical damage therefore a protective overlay in necessary. The optical properties of the protective overlay must be considered as to not interfere with the machine readable aspects designed into the Eclipse code. Since the Eclipse code is detected using optical detectors then the combination of the C-thru Holographic overlay, the eclipse code and the diversionary optical features must not interfere. This parameter in conjunction with the physical location of the eclipse code‘s location on the card is the only two constrains that the card designer must consider. The only other constraint is that the card is oriented correctly in the reader do so the Eclipse code is facing the optical detector. As in the case for magnetic stripe cards the physical magnetic stripe must be facing the sensor head for the card to be read. Same is true for our Eclipse code.

The next item on the list is the RFID inlay. The RFID chip may or may not be a smart chip. Using RFID inlay formed with a smart chip processor (such as DESFIRE) only adds additional levels of security to the stored data. The end user can choose the amount of security that is needed to keep the system as secure as required for the specific application.

Typically the inlay will be laminated between a series of materials constructed to have added durability. These layers then form a strong bond between the top and bottom surfaces of the cards and for a stress relieving intermediate layer to protect the RFID inlay as best as possible.

Figure 1 Components of the Hologram artwork

Figure 2 Composite drawing of the Hologram artwork

Once the structure of the card has been formed then the Hologram is hot-stamped on to the card surface. As mentioned previously the Hologram's artwork is designed in a wall paper fashion and the actual location of the covert machine readable features of the Hologram are "randomly placed" relative to the card surface hologram edge transition point. After the Hologram has been hot-stamped onto the cards surface the card is passed under a low power laser that has been temporarily programmed to ablate the Holographic material in a *random* pattern. Figure 3 shows an enlarged version of the Hologram and a typical random array of ablated hologram holes depicted as circles. The actual sizes of the geometric shapes depicted here are in the tens of microns so they are not readily visible as shown here. It is the combination of the independently formed laser ablated random pattern and the independently placed machine readable portion of the hologram that forms the basis of the Eclipse code. The cards are serialized, packaged and sent to the distribution center. At this point in the card manufacturing/issuing process these Eclipse patterns are still meaningless. The card manufacturer does not have or even given the know-how to complete the card.

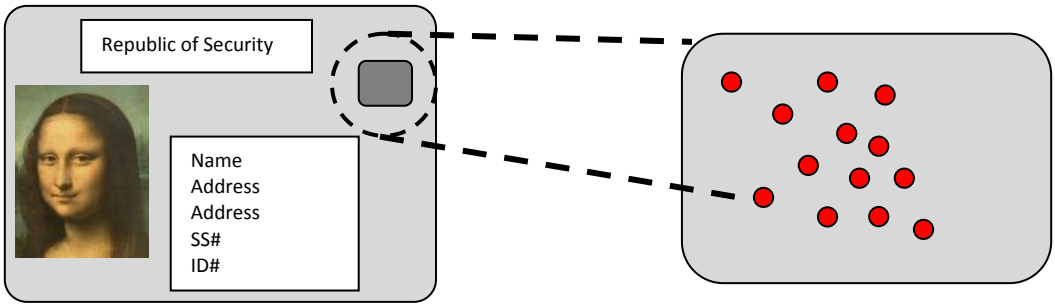

Figure 3 Expanded version of Eclipse Holographic optical code

Once the card is received at the distribution point the cards are ready to be personalized and distributed to the public. The eventual card holder goes to a distribution center where they are scanned for the particular biometric data to be stored on the card such as a fingerprint scan or a photo image or both. The biometric data is digitized and combined with additional information such as name and address etc.
To issue a card; the card is inserted into the specially designed issuing device and the optical detector within the reader will scan the Eclipse Code. Figure 4 shows the actual laser ablated random pattern as captured from the optical sensor. The second pattern read from the hologram is not shown. The two random patterns formed on the cards' surface are independently scanned and then mathematically convolved with each other. Then the information is then used to calculate a set of encryption keys that are then used to scramble the actual biometric and user information. All of that information is then stored in the cards' secure RFID memory. The Eclipse code system allows the agency to verify (1) the authenticity of the card and (2) the secure biometric data encrypted within the card is used to verify that the card holder is the correct person carrying the card.

What is shown in Figure 4 below is 15 random laser ablated optical marks formed in the hologram's surface. Once the card is inserted into the reader a microprocessor will detect the presence of the card and commence the illumination process of both independent codes. An area optical sensor will capture the image of the now first illuminated surface. Since the Eclipse code consists of two independent random optical codes then illumination process of detecting one portion of the code must not interfere with the scan of the other portion of the optical code. The illumination is changed and the same detector will then capture the next code. The optical detector we used in our prototype was a VGA sensor having 640 pixels in the x dimension and 480 pixels in the Y-dimension. The use of a higher pixel count sensor would provide additional security to the system, as described below.

The laser ablated holes as detected by the sensor cover an area of approximately 10 x 10 pixels, and the closest allowable hole to hole spacing is 6 pixels. That yields $\frac{640}{16} = 40$ possible hole locations in the X-dimension and $\frac{480}{16} = 30$ possible locations for holes in the Y-dimension. Therefore there are 40 x 30 = 1200 possible hole locations.

Based on the above conditions and the fact that the example give here uses n holes then the possible combinations C_n are:

$$Cn = \frac{1200!}{(1200 - n)!}$$

For an example of 10 holes the equation becomes

$$Cn = \frac{1200!}{(1200 - 10)!} = 5.9\ x\ 10^{30}$$

For then given example of 15 holes the equation becomes

$$Cn = \frac{1200!}{(1200 - 15)!} = 1.4\ x\ 10^{46}$$

For a 1.3Mega pixel optical sensor which is typically configured as 1280 x 1024 pixels then in the X-dimension there are $\frac{1280}{16} = 80$ possible locations and for the Y-dimension $\frac{1024}{16} = 64$ possible locations yielding 5120 possible laser ablated hole locations.

For an example of 10 holes the equation becomes

$$Cn = \frac{5120!}{(5120 - 10)!} = 1.22\ x\ 10^{37}$$

This configuration is equivalent to 100 bits encryption

For a configuration with 15 holes the equation becomes

$$Cn = \frac{5120!}{(5120 - 15)!} = 4.26\ x\ 10^{55}$$

this is approximately equivalent to 185 bits of encryption.

ZBA, Inc.
94 Old Camplain Road Hillsborough, NJ 08844
Ph: 908-359-2070 Fax: 908-595-0909
Web: http://www.zbausa.com/

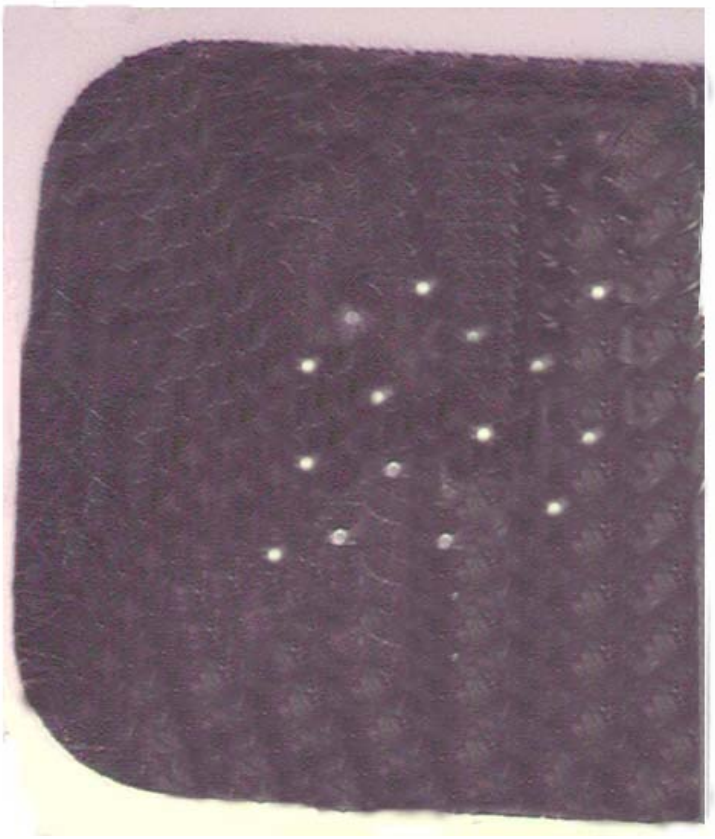

Figure 4 Image capture of the first random pattern

The calculations listed above represent only the first layer of defense against possible counterfeit. The calculations completely ignore the second random optical codes that are also scanned and are part of the calculations. Unlike a purely electronic encryption key the Eclipse code has two optical components that must be satisfied before the card can be accurately read.

Additionally, the prototype reader had a fingerprint sensor as part of the system. To speed up the verification process the fingerprint information is carried on the card. This eliminated the need for the system to connect via a secure intranet or internet connection to validate the fingerprint. Because the Eclipse code is extremely difficult crack then there is essentially no risk to carry the fingerprint data on the card. Once the fingerprint is captured then the microcontroller in the reader can performs the verification calculations. The next generation of Eclipse RFID cards/readers uses an embedded microcontroller on the cards so the verification of the fingerprint could be performed within the cards microcontrollers itself.

The reader is also protected in different ways to will ward off any unauthorized operator from using the reader as an issuance machine. The issuance reader is matched to the host PC. There is an electronic serial number associated with every reader and that serial number must match the numbers of an authentic manufactured reader. Additionally that particular reader can only be operated from the PC in which it is associated with. Additionally, there are only a few people that are authorized to use the reader as an issuance machine and they must carry an Eclipse cad to sign in including a biometric

verification. Only after the authorized user is enrolled can the issuance machine be operated. At that point the PC downloads a portion of the embedded program to the reader. This portion of the program is operating from Static RAM. This static RAM is specifically not battery backed-up. Should the reader and the PC be stolen from what should be a secure issuance location then once the reader is unplugged or powered off the reader will lose a critical part of it operating system and will not be able to re-start again unless the reboot process including the sign on by an authorized user is completed.

Summary

We have developed a secure ID card system that uses several layers of protection to prevent counterfeiting, modefieting, and genufeiting. The Eclipse system uses independent sets of randomly generated optical parameters to prevent any form of duplication. The Eclipse system when used in conjunction with a biometric completes the authentication process by a) the Eclipse code validates that the card is authentic, and b) the biometric validated the person using the card is authentic. The Eclipse system uses standard card manufacturing process and has little impact on the cost of the card.

Authors:

Victor Zazzu VP Engineering vicz@zbausa.com 908-359-2070	Wenyu Han President vivh@zbausa.com 908-359-2070

ZBA Inc
94 Old Camplain Road
Hillsborough, NJ 08844
www.zbausa.com

Appendix A Glossary of terms

Brute force Hacking = Describes a method in which a document ort ID cars is password protected. A fast computer is then programmed then programmed to sequentially cycle through all possible combination of codes until the correct password has been hit. For example a typical bank card uses a 4 digit PIN # to cycle through the 4 digits would only be 10^4 combinations, which is not much at all.

Counterfeiting= Originally produced document from other than the Authorized issuing Authority

Genufeiting = A document that reproduction (copy) using genuine material

Modifeting = A document that is altered at the time of issuance by the Authorized Issuing Authority.

HRI is an acronym of C-through hologram material manufactured by Crown Roll–Leaf Inc.

OVD An abbreviation for an Optically Variable Device

Match-on card: A technique used for fingerprint detection where the single users carries his fingerprint minutia on his/or hers respective card eliminating the need to perform a database look-up of many fingerprints.

Pixels: In digital imaging, a **pixel** (**pict**ure **el**ement) is the smallest piece of information in an image. Pixels are normally arranged in a regular 2-dimensional grid, and are often represented using dots or squares.

Laser Ablation: is the process of removing material from a solid (or occasionally liquid) surface by irradiating it with a laser beam. At low laser flux, the material is heated by the absorbed laser energy and evaporates or sublimates. At high laser flux, the material is typically converted to plasma.

Appendix B References:

1) **Wired Magazine May 2006 "The RFID Hacking Underground"** By Annalee Newitz
URL: http://www.wired.com/wired/archive/14.05/rfid.html

Appendix C Acknowledgements:

John Herslow of Composecure LLC. Whose help and advice was invaluable in getting our system designed and operational.

Composecure LLC is manufacturer of all types of ID cards for a variety of applications. They specialize in ID cards that comprise a multitude of different security features

James Kipp of Crown-Roll Leaf who supported us through a very intense design cycle and subsequently manufactured the Hologram used in this development.

Crown Roll-Leaf is an industry leading manufacturer of Holographic film for commercial and high security applications .

The above work is covered under several US and worldwide Patents.

ZBA, Inc.
94 Old Camplain Road Hillsborough, NJ 08844
Ph: 908-359-2070 Fax: 908-595-0909
Web: http://www.zbausa.com/